[1059] A hybrid access scheme, referred to as partial controlled access, provides the HSBS service as a subscription-based service that is encrypted with intermittent unencrypted advertisement transmissions. These advertisements may be intended to encourage subscriptions to the encrypted HSBS service. Scheduling of such unencrypted segments could be known to the MS through external means.

[1060] A wireless communication system 200 is illustrated in FIG. 3, wherein video and audio information is provided to Packetized Data Service Network (PDSN) 202 by a Content Server (CS) 201. The video and audio information may be from televised programming or a radio transmission. The information is provided as packetized data, such as in IP packets. The PDSN 202 processes the IP packets for distribution within an Access Network (AN). As illustrated the AN is defined as the portions of the system including a BS 204 in communication with multiple MS 206. The PDSN 202 is coupled to the BS 204. For HSBS service, the BS 204 receives the stream of information from the PDSN 202 and provides the information on a designated channel to subscribers within the system 200. To control the access, the content is encrypted by the CS 201 before being provided to the PDSN 202. The subscribed users are provided with the decryption key so that the IP packets can be decrypted.

[1061] FIG. 4 details an MS 300, similar to MS 206 of FIG. 3. The MS 300 has an antenna 302 coupled to receive circuitry 304. The MS 300 receives transmissions from a BS (not shown) similar to BS 204 of FIG. 3. The MS 300 includes a User Identification Module (UIM) 308 and a Mobile Equipment (ME) 306. The receive circuitry is coupled to the UIM 308 and the ME 306. The UIM 308 applies verification procedures for security of the HSBS transmission and provides various keys to the ME 306. The ME 306 may be coupled to processing unit 312. The ME 306 performs substantial processing, including, but not limited to, decryption of HSBS content streams. The ME 306 includes a memory storage unit, MEM 310. In the exemplary embodiment the data in the ME 306 processing unit (not shown) and the data in the ME memory storage unit, MEM 310 may be accessed easily by a non-subscriber by the use of limited resources, and therefore, the ME 306 is said to be insecure. Any information passed to the ME 306 or processed by the ME 306 remains

securely secret for only a short amount of time. It is therefore desired that any secret information, such as key(s), shared with the ME 306 be changed often.

[1062] The UIM 308 is trusted to store and process secret information (such as encryption keys) that should remain secret for a long time. As the UIM 308 is a secure unit, the secrets stored therein do not necessarily require the system to change the secret information often. The UIM 308 includes a processing unit referred to as a Secure UIM Processing Unit (SUPU) 316 and memory storage unit referred to as a Secure UIM Memory Unit (SUMU) 314 that is trusted to be secure. Within the UIM 308, SUMU 314 stores secret information in such a way as to discourage unauthorized access to the information. If the secret information is obtained from the UIM 308, the access will require a significantly large amount of resources. Also within the UIM 308, the SUPU 316 performs computations on values that may be external to the UIM 308 and/or internal to the UIM 308. The results of the computation may be stored in the SUMU 314 or passed to the ME 306. The computations performed with the SUPU 316 can only be obtained from the UIM 308 by an entity with significantly large amount of resources. Similarly, outputs from the SUPU 316 that are designated to be stored within the SUMU 314 (but not output to the ME 306) are designed such that unauthorized interception requires significantly large amount of resources. In one embodiment, the UIM 308 is a stationary unit within the MS 300. Note that in addition to the secure memory and processing within the UIM 308, the UIM 308 may also include non-secure memory and processing (not shown) for storing information including telephone numbers, e-mail address information, web page or URL address information, and/or scheduling functions, etc.

[1063] Alternate embodiments may provide a removable and/or reprogrammable UIM. In the exemplary embodiment, the SUPU 316 does not have significant processing power for functions beyond security and key procedures, wherein security and key procedures are typically may be used to allow encryption of the broadcast content of the HSBS. Alternate embodiments may implement a UIM having stronger processing power.

[1064] The UIM 308 is associated with a particular user and is used primarily to verify that the MS 300 is entitled to the privileges afforded the user, such as access to the mobile phone network. Therefore, a user is associated with the

UIM 308 rather than an MS 300. The same user may be associated with multiple UIM 308.

[1065] The broadcast service faces a problem in determining how to distribute keys to subscribed users. To decrypt the broadcast content at a particular time, the ME must know the current decryption key. To avoid theft-of-service, the decryption key should be changed frequently, for example, one service updates the key every minute. These decryption keys are called Short-term Keys (SK). The SK is used to decrypt the broadcast content for a short amount of time so the SK can be assumed to have some amount of intrinsic monetary value for a user. For example, this intrinsic monetary value may be a portion of the registration costs. Assume that the cost of a non-subscriber obtaining SK from the memory storage unit MEM 310 of a subscriber exceeds the intrinsic monetary value of SK. That is, the cost of illegitimately obtaining the SK exceeds the reward, resulting in no net benefit. Consequently, the need to protect the SK in the memory storage unit MEM 310 is reduced. However, if a secret key has a lifetime longer than that of the SK, the cost of illegitimately obtaining this secret key may actually be less than the reward. In this situation, there is a net benefit in illegitimately obtaining such a key from the memory storage unit MEM 310. Hence, ideally the memory storage unit MEM 310 will not store secrets with a lifetime longer than that of the SK.

[1066] The channels used by the CS (not shown) to distribute the SK to the various subscriber units are assumed to be insecure. In other words, an optimum design will assume the channels are insecure and design the SK accordingly. Therefore, when distributing a given SK, the CS desires to use a technique that hides the value of the SK from non-subscribed users. Furthermore, the CS distributes the SK to each of a potentially large number of subscribers for processing in respective MEs within a relatively short timeframe. Known secure methods of key transmission are traditionally slow and require transmission of a large number of keys. Key transmission methods are generally not feasible for the desired combination of security and efficiency criteria. The exemplary embodiment is a feasible method of distributing decryption keys to a large set of subscribers within a small time-frame in such a way that non-subscribers cannot obtain the decryption keys.

[1067] The exemplary embodiment is described as transmitting the information in Internet Protocol compatible packets, such as "IPSec" packets as described hereinbelow, and therefore, the following description provides a brief introduction to terminology used in association with IPSec. This terminology is useful for describing exemplary embodiments, but the use of this terminology is not meant to limit the exemplary embodiment to communications using IPSec.

[1068] The foundations of IPSec are specified in RFC 1825 entitled "Security Architecture for the Internet Protocol" by R. Atkinson in August 1995, RFC 1826 entitled "IP Authentication Header" by R. Atkinson in August 1995, and RFC 1827 entitled "IP Encapsulating Security Payload (ESP)" by R. Atkinson in August 1995. The authentication header is a mechanism for providing integrity to IP datagrams, wherein IP datagrams are generally a collection of useful information, referred to as a *payload*, combined with network control information and an IP header. Network routers use the IP header to direct the packet to the proper network node. In some circumstances, the authentication header may also provide authentication to IP datagrams. ESP is a mechanism for providing confidentiality and integrity to IP datagrams, and may be used in conjunction with the authentication header. IPSec utilizes "security associations" to describe the parameters, such as the encryption key and encryption algorithm, used to encrypt and/or authenticate communications between a group of entities. Note that the concept of a security association is also valid when applied to cryptosystems not based on IPSec.

[1069] An IPSec packet includes a 32-bit parameter called the Security Parameter Index (SPI) that is used, in conjunction with the destination address, to identify the security association used to encrypt and/or authenticate the contents of the IP datagram. An entity may store the security associations in a security association database and index the security associations according to the Destination Address and SPI. The encrypted contents of an IPSec packet are often called the payload.

[1070] In the exemplary embodiment, the MS 300 supports HSBS in a wireless communication system. To obtain access to HSBS, the user must register and then subscribe to the service. Once the subscription is enabled, the various keys are updated as required. In the registration process the CS

and UIM 308 negotiate a security association, and agree on a Registration Key (RK) and other parameters required for the security association between the user and the CS. The CS may then send the UIM 308 further secret information encrypted with the RK. The RK is kept as a secret in the UIM 308, while other parameters may be kept in the ME 306. The RK is unique to a given UIM 308, i.e., each user is assigned a different RK. The registration process alone does not give the user access to HSBS.

[1071] As stated hereinabove, after registration the user subscribes to the service. In the subscription process the CS sends the UIM 308 the value of a common Broadcast Access Key (BAK). Note that while the RK is specific to the UIM 308, the BAK is used to encrypt a broadcast message to multiple users. The CS sends the MS 300, and specifically UIM 308, the value of BAK encrypted using the RK unique to UIM 308. The UIM 308 is able to recover the value of the original BAK from the encrypted version using the RK. The BAK, along with other parameters, form a security association between the CS and the group of subscribed users. The BAK is kept as a secret in the UIM 308, while other parameters of the security association may be kept in the ME 306. The CS then broadcasts data called SK Information (SKI) that is combined with the BAK in the UIM 308 to derive SK. The UIM 308 then passes SK to the ME 306. In this way, the CS can efficiently distribute new values of SK to the ME of subscribed users. Presented hereinbelow are several examples of how SK is derived from SKI, and the forms that SKI may take. The registration and subscription processes are discussed in detail, after which the SKI and SK are described.

[1072] With respect to registration, when a user registers with a given CS, the UIM 308 and the CS (not shown) set-up a security association. That is, the UIM 308 and the CS agree on a secret registration key RK. The RK is unique to each UIM 308, although if a user has multiple UIMs then these UIMs may share the same RK dependent on the policies of the CS. This registration may occur when the user subscribes to a broadcast channel offered by the CS or may occur prior to subscription. A single CS may offer multiple broadcast channels. The CS may choose to associate the user with the same RK for all channels or require the user to register for each channel and associate the same user with

different RKs on different channels. Multiple CSs may choose to use the same registration keys or require the user to register and obtain a different RK for each CS.

[1073] Three common scenarios for setting up this security association include: 1) the Authenticated Key Agreement (AKA) method which is used in 3GPP systems; 2) the Internet Key Exchange (IKE) method as used in IPSec; and 3) Over-The-Air-Service-Provisioning (OTASP). In either case the UIM memory unit SUMU 314 contains a secret key referred to herein as the A-key. For example, using the AKA method, the A-key is a secret known only to the UIM and a Trusted Third Party (TTP), wherein the TTP may consist of more than one entity. The TTP is typically the mobile service provider with whom the user is registered. All communication between the CS and TTP is secure, and the CS trusts that the TTP will not assist unauthorized access to the broadcast service. When the user registers, the CS informs the TTP that the user wishes to register for the service and provides verification of the user's request. The TTP uses a function, similar to a cryptographic hash function, to compute the RK from the A-key and additional data called Registration Key Information (RKI). The TTP passes RK and/or RKI to the CS over a secure channel along with other data. The CS sends RKI to the MS 300. The receiver circuitry 304 passes RKI to the UIM 308 and may pass RKI to the ME 306. The UIM 308 computes RK from RKI and the A-key that is stored in the UIM memory unit SUMU 314. The RK is stored in the UIM memory unit SUMU 314 and is not provided directly to the ME 306. Alternate embodiments may use an IKE scenario or some other method to establish the RK. The other parameters of the security association between the CS and UIM 308 must also be negotiated. The RK is kept as a secret in the UIM 308, while other parameters of the security association may be kept in the ME 306. In the exemplary embodiment, in which BAK is sent to the UIM 308 as an IPSec packet encrypted using RK, the CS and MS 300 negotiate a value of SPI used to index the security association and this SPI is denoted SPI_RK.

[1074] In the AKA method, the RK is a secret shared between the CS, UIM and TTP. Therefore, as used herein, the AKA method implies that any security association between the CS and UIM implicitly includes the TTP. The inclusion

of the TTP in any security association is not considered a breach of security as the CS trusts the TTP not to assist in unauthorized access to the broadcast channel. As stated hereinabove, if a key is shared with the ME 306, it is desirable to change that key often. This is due to the risk of a non-subscriber accessing information stored in memory storage unit MEM 310 and thus allowing access to a controlled or partially controlled service. The ME 306 stores SK, i.e., key information used for decrypting broadcast content, in memory storage unit MEM 310. The CS sends sufficient information for subscribed users to compute SK. If the ME 306 of a subscribed user could compute SK from this information, then additional information required to compute SK cannot be secret. In this case, assume that the ME 306 of a non-subscribed user could also compute SK from this information. Hence, the value of SK must be computed in the SUPU 316, using a secret key shared by the CS and SUMU 314. The CS and SUMU 314 share the value of RK, however each user has a unique value of RK. There is insufficient time for the CS to encrypt SK with every value of RK and transmit these encrypted values to each subscribed user.

[1075] With respect to subscription, to ensure the efficient distribution of the security information SK, the CS periodically distributes a common Broadcast Access Key (BAK) to each subscriber UIM 308. For each subscriber, the CS encrypts BAK using the corresponding RK to obtain a value called BAKI Information (BAKI). The CS sends the corresponding BAKI to MS 300 of the subscribed user. For example, BAK may be transmitted as an IP packet encrypted using the RK corresponding to each MS. In the exemplary embodiment, BAKI is an IPSec packet containing BAK that is encrypted using RK as the key. Since RK is a per-user key, the CS must send the BAK to each subscriber individually; thus, the BAK is not sent over the broadcast channel. The MS 300 passes the BAKI to the UIM 308. The SUPU 316 computes BAK using the value of RK stored in SUMU 314 and the value of BAKI. The value of BAK is then stored in the SUMU. In the exemplary embodiment, the BAKI contains a SPI value denoted SPI_RK that corresponds to the security association that contains RK. The MS 300 knows that the UIM 308 can decrypt the payload when the IPSec packet is encrypted according to this security

association. Consequently, when the MS 300 receives an IPSec packet encrypted according to this security association, MS 300 passes BAKI to the UIM 308, and instructs the UIM 308 to use the RK to decrypt the payload.

[1076] The period for updating the BAK is desired to be sufficient to allow the CS to send the BAK to each subscriber individually, without incurring significant overhead. Since the ME 306 is not trusted to keep secrets for a long time, the UIM 308 does not provide the BAK to the ME 306. The other parameters of the security association between the CS and group of subscribers must also be negotiated. In one embodiment, these parameters are fixed, while in another embodiment, these parameters may be sent to the MS as part of the BAKI. While the BAK is kept as a secret in the UIM 308, other parameters of the security association may be kept in the ME 306. In one embodiment, in which SK is sent to the MS 300 as an IPSec packet encrypted using BAK, the CS provides the subscribers with an SPI used to index the security association and this SPI is denoted SPI_BAK.

[1077] The following paragraph discusses how the SK is updated following a successful subscription process. Within each period for updating the BAK, a short-term interval is provided during which SK is distributed on a broadcast channel. The CS uses a cryptographic function to determine two values SK and SKI (SK Information) such that SK can be determined from BAK and SKI. For example, SKI may be the encryption of SK using BAK as the key. In one exemplary embodiment, SKI is an IPSec packet in which the payload contains the value of SK encrypted using BAK as the key. Alternatively, SK may be the result of applying a cryptographic hash function to the concatenation of the blocks SKI and BAK. The CS ideally ensures that the values of SK cannot be predicted in advance. If SK can be predicted in advance, then an attacker, i.e., illegitimate accessing entity, can send the predicted values of SK to un-subscribed users.

[1078] As an example, suppose *N* values of SK are to be used over a 24-hour period. If SK is predicted with 100% accuracy, the attacker need only ask the UIM to compute the *N* keys. The attacker then makes the *N* keys available to un-subscribed users. The un-subscribed users can download the keys at the beginning of each day and access the HSBS service with little cost or

inconvenience. If the attacker is only able to predict SK with 50% accuracy, then the attacker needs to send approximately *2N* keys. As the accuracy of the predictions decreases, the number of keys to be generated by the attacker increases. An attacker can be dissuaded from distributing the predictions to SK by ensuring that the cost of generating, storing and distributing the predictions exceeds the benefit of providing illegitimate access. Attackers may be discouraged by ensuring that the accuracy of any prediction by the attacker is sufficiently small, thus increasing the number of keys the attacker will generate to the point where the cost of providing illegitimate access exceeds the benefit. Consequently, any scheme for generating SK ideally ensures that the best predictions of an attacker have sufficiently small accuracy. That is, the computation of SK should include some random value that can only be predicted in advance with small accuracy.

[1079] In an exemplary embodiment where SK is in an encrypted form, the CS can choose SK using a random or pseudo-random function. In alternate embodiments, wherein SK is derived by applying a cryptographic function to SKI and BAK, the CS introduces an unpredictable value when forming SKI. Some portion of SKI may be predictable. For example, a portion of SKI may be derived from the system time during which this SKI is valid. This portion, denoted SKI_PREDICT, may not be transmitted to the MS 300 as part of the broadcast service. The remainder of SKI, SKI_RANDOM may be unpredictable. That is, SK_RANDOM is predicted with small accuracy. The SKI_RANDOM is transmitted to the MS 300 as part of the broadcast service. The MS 300 reconstructs SKI from SKI_PREDICT and SKI_RANDOM and provides SKI to UIM 308. The SKI may be reconstructed within the UIM 308. The value of SKI changes for each new SK. Thus, either SKI_PREDICT and/or SKI_RANDOM changes when computing a new SK.

[1080] The CS sends SKI_RANDOM to BS for broadcast transmission. The BS broadcasts SKI_RANDOM, which is detected by the antenna 302 and passed to the receive circuitry 304. Receive circuitry 304 provides SKI_RANDOM to the MS 300, wherein the MS 300 reconstructs SKI. The MS 300 provides SKI to UIM 308, wherein the UIM 308 obtains the SK using the BAK stored in SUMU 314. The SK is then provided by UIM 308 to ME 306.

The ME 306 stores the SK in memory storage unit, MEM 310. The ME 306 uses the SK to decrypt broadcast transmissions received from the CS.

[1081] The CS and BS agree on some criteria for when SKI_RANDOM is to be transmitted. The CS may desire to reduce the intrinsic monetary value in each SK by changing SK frequently. In this situation, the desire to change SKI_RANDOM data is balanced against optimizing available bandwidth. In some exemplary embodiments, SKI_RANDOM is sent with the encrypted content. This allows the MS 300 to generate SK and start decrypting immediately. In many situations, this will waste bandwidth. An exception is a scheme in which SKI_RANDOM is sent as parameters of the communication. For example, the SPI value in IPSec is allowed to vary, and can be exploited to include an SKI_RANDOM value, as discussed in further detail hereinbelow.

[1082] In other embodiments, SKI_RANDOM is sent separate from the encrypted content. The SKI_RANDOM may even be transmitted on a channel other than the broadcast channel. When a user "tunes" to the broadcast channel, the receive circuitry 304 obtains information for locating the broadcast channel from a "control channel." It may be desirable to allow quick access when a user "tunes" to the broadcast channel. This requires the ME 306 to obtain SKI within a short amount of time. The ME 306 may already know SKI_PREDICT, however, the BS provides SKI_RANDOM to ME 300 within this short amount of time. For example, the BS may frequently transmit SKI_RANDOM on the control channel, along with the information for locating the broadcast channel, or frequently transmit SKI_RANDOM on the broadcast channel. The more often that the BS "refreshes" the value of SKI_RANDOM, the faster the MS 300 can access the broadcast message. The desire to refresh SKI_RANDOM data is balanced against optimizing available bandwidth, as transmitting SKI_RANDOM data too frequently may use an unacceptable amount of bandwidth in the control channel or broadcast channel.

[1083] In some situations the CS may choose to use values of SKI_PREDICT and SKI_RANDOM wherein both change for every value of SK produced. In other situations the CS may wish to reduce the number of times that SKI_RANDOM changes, so that the MS 300 does not have to obtain SKI_RANDOM so often. For example, if a user changes frequently between

multiple HSBS channels, then it would be better if the value of SKI_RANDOM were unlikely to change in the five minutes during which the user is tuned to another channel. If SKI_RANDOM changed then the user would have to wait until the new value of SKI_RANDOM is broadcast, indicating that such a scheme would be more "user-friendly" if SKI_RANDOM remains constant for as long as possible. The CS may wish to use multiple values of SK during the lifetime of an SKI_RANDOM value, by using a value for SKI_PREDICT that will have changed whenever the CS wishes to change SK. One example uses system time; however, using system time introduces additional problems regarding synchronization.

[1084] With respect to encryption and transmission of the broadcast content, the CS encrypts the broadcast content using the current SK. The exemplary embodiment employs an encryption algorithm such as the Advanced Encryption Standard (AES) Cipher Algorithm. In the exemplary embodiment, the encrypted content is then transported by an IPsec packet according to the Encapsulating Security Payload (ESP) transport mode discussed hereinbelow. The IPsec packet also contains an SPI value that instructs the ME 306 to use the current SK to decrypt received broadcast content. The encrypted content is sent via the broadcast channel.

[1085] Receive circuitry 304 provides the RKI and BAKI directly to the UIM 308. Further, if the CS computes SK from SKI_RANDOM and SKI_PREDICT values, then receive circuitry 304 provides the SKI_RANDOM to an appropriate part of the MS 300 where it is combined with SKI_PREDICT to obtain SKI. In one embodiment, SKI is attached to the encrypted message, and is extracted by the ME 306. The SKI is provided to the UIM 308 by the relevant part of the MS 300. The UIM 308 computes RK from the RKI and A-key, decrypts the BAKI using the RK to obtain BAK, and computes the SK using the SKI and BAK, to generate an SK for use by the ME 306. The ME 306 decrypts the broadcast content using the SK. The UIM 308 of the exemplary embodiment may not be sufficiently powerful for decryption of broadcast content in real time, and, therefore, SK is passed to the ME 306 for decrypting the broadcast.

[1086] FIG. 5B illustrates the transmission and processing of keys, including RK, BAK and SK, according to an exemplary embodiment. As illustrated, at

registration, the MS 300 receives the RK Information (RKI) and passes it to UIM 308, wherein the SUPU 316 computes RK using RKI and the A-key, and stores the RK in UIM memory storage SUMU 314. The MS 300 periodically receives the BAK Information (BAKI) that contains BAK encrypted using the RK value specific to UIM 308. The encrypted BAKI is decrypted by SUPU 316 to recover the BAK, which is stored in UIM memory storage SUMU 314. The MS 300 further periodically obtains SKI. In some exemplary embodiments, the MS 300 receives an SKI_RANDOM that it combines with SKI_PREDICT to form SKI. The SUPU 316 computes SK from SKI and BAK. The SK is provided to ME 306 for decrypting broadcast content.

[1087] In the exemplary embodiment the CS keys are not necessarily encrypted and transmitted to the MSs; the CS may use an alternative method. The key information generated by the CS for transmission to each MS provides sufficient information for the MS to calculate the key. As illustrated in the system 350 of FIG. 6, the RK is generated by the CS, but RK Information (RKI) is transmitted to the MS. The CS sends information sufficient for the UIM to derive the RK, wherein a predetermined function is used to derive the RK from transmitted information from the CS. The RKI contains sufficient information for the MS to determine the original RK from the A-key and other values, such as system time, using a predetermined public function labeled d1, wherein:

$$RK = d1(A\text{-key}, RKI). \quad (3)$$

[1088] In the exemplary embodiment, the function d1 defines a cryptographic-type function. According to one embodiment, RK is determined as:

$$RK = SHA'(A\text{-key} \,||\, RKI), \quad (4)$$

wherein "||" denotes the concatenation of the blocks containing A-key and RKI, and SHA'(X) denotes the last 128-bits of output of the Secure Hash Algorithm SHA-1 given the input X. In an alternative embodiment, RK is determined as:

$$RK = AES(A\text{-key}, RKI), \quad (5)$$

wherein AES(X,Y) denotes the encryption of the 128-bit block RKI using the 128-bit A-key. In a further embodiment based on the AKA protocol, RK is determined as the output of the 3GPP key generation function *f3*, wherein RKI

includes the value of RAND and appropriate values of AMF and SQN as defined by the standard.

[1089] The BAK is treated in a different manner because multiple users having different values of RK must compute the same value of BAK. The CS may use any technique to determine BAK. However, the value of BAKI associated with a particular UIM 308 must be the encryption of BAK under the unique RK associated with that UIM 308. The SUPU 316 decrypts BAKI using RK stored in the SUMU 314 according to the function labeled d2, according to:

$$BAK = d2(BAKI, RK). \quad (6)$$

[1090] In an alternate embodiment, the CS may compute BAKI by applying a decryption process to BAK using RK, and the SUPU 316 obtains BAK by applying the encryption process to BAKI using RK. This is considered equivalent to the CS encrypting BAK and the SUPU 316 decrypting BAKI. Alternate embodiments may implement any number of key combinations in addition to or in place of those illustrated in FIG. 6.

[1091] The SK is treated in a similar manner to RK. In some embodiments, SKI is first derived from the SKI_PREDICT and SKI_RANDOM, wherein SKI_RANDOM is the information transmitted from CS to MS. Then a predetermined function labeled d3 is used to derive the SK from SKI and BAK (stored in the SUMU 314), according to:

$$SK = d3(BAK, SKI). \quad (7)$$

[1092] In one embodiment, the function d3 defines a cryptographic-type function. In an exemplary embodiment, SK is computed as:

$$SK = SHA(BAK \,||\, SKI), \quad (8)$$

while in another embodiment, SK is computed as

$$SK = AES(BAK, SKI). \quad (9)$$

[1093] A method of providing the security for a broadcast message is illustrated in FIGs. 7A-7D. FIG. 7A illustrates a registration process 400 wherein a subscriber negotiates registration with the CS at step 402. The registration at step 404 provides the UIM a unique RK. The UIM stores the RK in a Secure Memory Unit (SUMU) at step 406. FIG. 7B illustrates subscription processing 420 between a CS and a MS. At step 422 the CS generates a BAK for a BAK time period T1. The BAK is valid throughout the BAK time period T1,

wherein the BAK is periodically updated. At step 424 the CS authorizes the UIM to have access to the Broadcast Content (BC) during the BAK timer period T1. At step 426 the CS encrypts the BAK using each individual RK for each subscriber. The encrypted BAK is referred to as the BAKI. The CS then transmits the BAKI to the UIM at step 428. The UIM receives the BAKI and performs decryption using the RK at step 430. The decrypted BAKI results in the originally generated BAK. The UIM stores the BAK in a SUMU at step 432.

[1094] When the user subscribes to the broadcast service for a particular BAK update period, the CS sends the appropriate information BAKI, wherein BAKI corresponds to the BAK encrypted with the RK. This typically occurs prior to the beginning of this BAK update period or when the MS first tunes to the broadcast channel during this BAK update period. This may be initiated by the MS or CS according to a variety of criteria. Multiple BAKI may be transmitted and decrypted simultaneously.

[1095] Note that when expiration of the BAK update period is imminent, the MS may request the updated BAK from the CS if the MS has subscribed for the next BAK update period. In an alternate embodiment the first timer t1 is used by the CS, where upon expiration of the timer, i.e., satisfaction of the BAK update period, the CS transmits the BAK. The CS may change the value of BAK earlier than originally intended. This may be desirable if, for example, the current value of BAK is publicly disclosed.

[1096] Note that it is possible for a user to receive a BAK during a BAK update period, wherein, for example, a subscriber joins the service mid-month when the BAK updates are performed monthly. Additionally, the time periods for BAK and SK updates may be synchronized, such that all subscribers are updated at a given time.

[1097] FIG. 8A illustrates the registration process in a wireless communication system 500 according to the exemplary embodiment. The CS 502 negotiates with each subscriber, i.e., MS 512, to generate a specific RK to each of the subscribers. The RK is provided to the SUMU unit within the UIM of each MS. As illustrated, the CS 502 generates RK_1 that is stored in $SUMU_1$ 510 within UIM_1 512. Similarly, the CS 502 generates RK_2 and RK_N which are

stored in $SUMU_2$ 520 within UIM_2 522 and $SUMU_N$ 530 within UIM_N 532, respectively.

[1098] FIG. 8B illustrates the subscription process in the system 500. The CS 502 further includes multiple encoders 504. Each of the encoders 504 receives one of the unique RKs and the BAK value generated in the CS 502. The output of each encoder 504 is a BAKI encoded specifically for a subscriber. The BAKI is received at the UIM of each MS, such as UIM_1 512. Each UIM includes a SUPU and a SUMU, such as $SUPU_1$ 514 and $SUMU_1$ 510 of UIM_1 512. The SUPU includes a decoder, such as decoder 516 that recovers the BAK by application of the RK of the UIM. The process is repeated at each subscriber.

[1099] FIG. 8D illustrates the processing of BC after registration and subscription. The CS 502 includes an encoder 560 that encodes the BC using the current SK to generate the EBC. The EBC is then transmitted to the subscribers. Each MS includes an encoder, such as encoder 544, that extracts the BC from the EBC using the SK.

[1100] The following description considers four exemplary embodiments that may be used to update SK and broadcast the content. In the first exemplary embodiment, SK is derived from BAK and the SPI value in the header of the IPSec packets containing the broadcast content. In the second exemplary embodiment, SK is derived from BAK, a broadcast random value denoted RAND and the SPI value in the header of the IPSec packets containing the broadcast content. In the third exemplary embodiment, SK is derived from BAK, system time and a broadcast random value denoted SK_RAND. In the fourth exemplary embodiment, SK is sent as an IPSec packet encrypted using BAK. Still further embodiments may provide SK as a combination of the above listed embodiments, or using another mechanism to provide the SK to the MS often enough to discourage unauthorized access to the broadcast service.

[1101] As the Short-term Key (SK) is used to encrypt and decrypt the broadcast content, and is stored in memory that may be vulnerable to unauthorized access, wherein the SK is typically changed frequently. A problem exists as to how to change the SK frequently while balancing the following four objectives: 1) to minimize the SK update waiting time or blackout

period, for a mobile station that has recently tuned to the broadcast; 2) to minimize the amount of bandwidth used to update the SK value; 3) to increase the level of security; and 4) to increase the ease with which the SK can be incorporated with IPSec. Frequent updates may reduce the blackout period but at the expense of requiring more bandwidth to send frequent updates.

[1102] One solution provides a method for providing sufficient information for performing SK updates in each encrypted broadcast content packet without using any additional bandwidth. Therefore, the blackout period may be minimized without necessarily incurring additional bandwidth requirements. The four exemplary embodiments described herein for performing an SK update have various advantages and disadvantages. All four embodiments provide methods that are sufficiently secure. The first embodiment eliminates the block out period and uses no additional bandwidth to update the SK value. The other embodiments may incur a blackout period during times of high usage. The first embodiment is also easily incorporated with IPSec.

[1103] According to the first embodiment for performing an SK update, the above mentioned problems are solved by defining the SK that encrypts a given IPSec packet as a function of the Broadcast Access Key (BAK) and the SPI in the ESP header. In this way, rather than providing the SK in a separate stream, the SK is computed from the content stream. Assuming that the MS has already received the BAK as described hereinabove, the MS is able to immediately compute the SK for each content packet without having to wait for some additional SK update information. This effectively eliminates any SK update wait time for a new broadcast recipient. As soon as the MS receives a content packet, the MS can immediately determine the SK and decrypt the content.

[1104] Information sufficient to calculate the SK at the MS is provided in the IPSec packet. The IPSec packet utilizes an IP Encapsulating Security Payload (ESP) and is specified in RFC 1827 entitled "IP Encapsulating Security Payload (ESP)" by R. Atkinson in August 1995, as mentioned above herein. ESP is a mechanism for providing integrity and confidentiality to IP datagrams. In some circumstances it can also provide authentication to IP datagrams. FIG. 9A illustrates an IPSec packet 600, including an IP header 602, an ESP header

604, and a payload 606, according to one embodiment. The Encapsulating Security Payload (ESP) may appear anywhere after the IP header and before the final transport-layer protocol. Generally, the ESP consists of an unencrypted header followed by encrypted data.

[1105] The ESP header field 604 includes a Security Association Identifier, referred to as the SPI. According to the first embodiment described hereinabove, the IPSec packets containing the broadcast content include an SPI related to the SK, labeled SPI_SK. FIG. 9B illustrates the format of the corresponding 32-bit SPI_SK 610. The SPI_SK 610 is decomposed into two parts: SPI_RAND 612 and BAK_ID 614. The SPI_RAND 612 is a random number that is statistically random, and is also used to compute the SK that is used to encrypt and decrypt the corresponding broadcast content or payload. The SPI_RAND parameter allows the Content Server (CS) to frequently change the effective SK value for the content by changing the SPI_RAND value, thus providing the MS the parameter needed to compute the SK value immediately. Furthermore, SPI_RAND fulfills the role of SKI_RANDOM, discussed hereinabove. The randomness of SPI_RAND ensures that an attacker cannot predict the values of SK with high accuracy. Since the SPI is already a standard parameter in IPSec encrypted packets, i.e., is specified for the ESP, the present embodiment does not incur the additional bandwidth typically associated with transmitting the SK as a separate stream. The BAK_ID indicates which BAK value to use for computation of the SK value. In one embodiment the BAK_ID is a four bit tag, wherein each tag is associated with a BAK value. When the MS performs a subscription, the MS stores each received BAK_ID and the corresponding BAK value in a memory storage unit. According to one embodiment the MS includes a Look Up Table (LUT) for storing the BAK value(s) identified with each corresponding BAK_ID(s). The BAK LUT is contained in the secure memory in the UIM.

[1106] FIG. 9D illustrates a BAK LUT 630. Each entry in the LUT 630 identifies the BAK_ID, the corresponding BAK value, and the expiration of the validity of the combination. The expiration is introduced due to the small number of values of BAK_ID. Alternate embodiments may avoid the use of expiration values in the BAK LUT. In one embodiment, only 16 values of

BAK_ID are used. If a new BAK is issued every month, then the value of BAK_ID must repeat after 16 months. At that time, there may be confusion as to which value of BAK is valid. The expiration provides a time-out period after which a new entry replaces the expired entry. The BAK LUT may need to store more than one value of BAK. One reason for this is that the CS may wish to send BAK values to the MS before they become valid. Additionally, the CS may wish to have multiple BAK values that are valid at the same time, wherein different BAK values may be used to compute different SK values. If the BAK LUT does not contain a current BAK corresponding to the BAK_ID, then the MS may perform a subscription to retrieve the valid BAK.

[1107] After extracting SPI_RAND and BAK_ID from the SPI_SK, and retrieving BAK corresponding to BAK_ID, the UIM computes the value of SK from BAK and SPI_RAND using a cryptographic function *g*:

$$SK = g(\text{BAK}, \text{SPI\_RAND}). \quad (10)$$

[1108] In one embodiment, the function g(BAK, SPI_RAND) corresponds to encryption of SPI_RAND padded to 128-bit bits with zeroes, using the AES encryption algorithm with BAK as the key:

$$SK = \text{AES}(\text{BAK}, \text{SPI\_RAND}). \quad (11)$$

[1109] In another embodiment, the function g(BAK, SPI_RAND) corresponds to computing the 128 least significant bits of the output of SHA-1 applied to the concatenation of BAK and SPI_RAND:

$$SK = \text{SHA}(\text{BAK}, \text{SPI\_RAND}). \quad (12)$$

[1110] In this way, it is not necessary for the UIM to compute the value of SK for each packet received by the MS. The MS stores each of the SPI_SK values with the corresponding SK values in a memory storage unit, such as a Look Up Table (LUT). The MS may store the SPI_SK and SK values as a security association in the Security Association Database (SAD): an LUT in which the MS stores typical security associations required for other applications. The security associations are indexed according to the destination address and SPI. When a new SK is generated from a new value of SPI_SK, the old security association is replaced by the new security association containing the new values of SPI_SK and SK. Alternatively, the MS may store the SPI_SK and SK values in a SK_LUT, with one SK_LUT allocated to each broadcast channel.

FIG. 9C illustrates an SK LUT 620. Each entry in the LUT 620 identifies the SPI_SK and the corresponding SK value. When the MS receives a broadcast content packet, the ME first checks the SAD or SK LUT to see if the table contains an SPI_SK value equal to the SPI of the received packet. If the table contains such a value, then the ME uses this value, otherwise the UIM computes the new value of SK. The CS may also have a BAK LUT, SAD or SK_LUT.

[1111] FIGs. 10 and 11 illustrate one embodiment for performing an SK update. FIG. 10 illustrates method 700 of operation of the CS. For each IP packet, the CS determines the BAK that will be used to derive SK, and determines the BAK_ID corresponding to the BAK at step 702. The BAK_ID may be any type of identifier that allows discrimination among multiple BAK values. The CS sends BAK and the BAK_ID to individual users by performing subscription at step 706. The users may perform subscription at various times before and during the subscription period. Steps 702 and 706 may occur before the subscription period starts. At step 710 the CS chooses a random value for the SPI_RAND value. If the BAK_ID is represented using *b* bits, then the SPI_RAND is represented using (32-*b*) bits. The SPI_RAND value should not be repeated during the lifetime of one BAK. Once the SPI_RAND and BAK_ID are known, the CS combines them (i.e., concatenates BAK_ID to the SPI_RAND) to form the SPI_SK at step 712. At step 714, the CS forms SK by using a cryptographic function to combine SPI_RAND with the BAK corresponding to BAK_ID to form SK. The CS then encrypts the broadcast message or portion of the message with SK at step 716, and sends the encrypted message at step 718. Note that the encrypted broadcast message is part of an IP packet that includes the IP header and the ESP header. The ESP header includes the SPI_SK. At decision diamond 720, the CS decides whether to change SK. If the CS decides not to change SK, then the CS proceeds to step 716. If the CS decides to change SK, then the CS proceeds to decision diamond 724, where the CS decides whether to change BAK. If the CS decides not to change BAK, then the CS proceeds to step 710. If the CS decides to change BAK, then the CS proceeds to step 702.

[1112] FIG. 11 illustrates the corresponding operation at the receiver, such as a MS. The method 750 initiates when the receiver receives the IP packet including the SPI_SK in the ESP header at step 752. Note that the receiver extracts the SPI_SK information from the IP packet. Upon receipt of the SPI_SK, the receiver first checks if the SK corresponding to the received SPI_SK value is stored in memory.

[1113] In one embodiment, the SPI_SK is stored in an SK LUT stored in the ME 306 unit of FIG. 4 and in another embodiment, the SPI_SK is stored in the security association database: both of these tables are denoted in FIG. 11 by SPI table. The check of the SPI table is performed at decision diamond 754. If the SK value is stored in memory at the receiver, the receiver is able to decrypt the payload of the content packet using the stored SK value at step 756. If the receiver does not have the SK value stored in memory, the receiver extracts BAK_ID and SPI_RAND from SPI_SK at step 758. At Step 760, the receiver then checks if the BAK LUT has a valid BAK entry corresponding to BAK_ID. If the BAK LUT does have a valid BAK corresponding to BAK_ID, then the receiver selects this value and proceeds to step 764. If the BAK LUT does not have a valid BAK corresponding to BAK_ID, such as when the user wishes to subscribe for this period, then the receiver performs a subscription to obtain the valid BAK as shown at step 762. The new BAK is stored with BAK_ID in the BAK_LUT and the receiver proceeds to step 764. The receiver combines the BAK corresponding to the BAK_ID value, i.e., BAK_ID in the received SPI_SK, and the SPI_RAND value (also in the received SPI_SK) to compute the new SK at step 764. The receiver then uses the new SK value to decrypt the payload of the content packet at step 766. The receiver also stores this SK value indexed by the corresponding SPI_SK and possibly the destination address of the IPSec packets.

[1114] The SK is computed directly from knowledge of the BAK and the SPI_SK value in the content packet. The BAK changes less frequently than the SK, e.g., BAK may change once a month. Therefore, the receiver is able to determine the SK value immediately from the content packets without additional delay and without requiring more bandwidth to send the SK update.

[1115] According to one embodiment, the SK calculation is given as:

$$SK=f(SPI\_SK, BAK), \quad (13)$$

wherein the function is defined as encryption of the SPI_SK using the BAK. As the SPI_SK is made up of the SPI_RAND and the BAK_ID, Equation (13) may also be given as:

$$SK=f(SPI\_RAND, BAK\_ID). \quad (14)$$

[1116] The second exemplary embodiment for performing an SK update introduces an additional aspect of randomness to the computation of SK, wherein SK is defined as a function of BAK, SPI_RAND, and an additional parameter, RAND. The RAND parameter is kept constant for several SK values. The RAND allows more different values of SK to be derived from a single BAK value by changing both SPI_RAND and RAND. If no RAND is used then there are at most 2^{32} values of SK that can be derived from a single BAK by varying the SPI. However, if a 96-bit RAND is used, then there can be up to 2^{218} values of SK that can be derived from a single BAK by varying both SPI_RAND and RAND. (These numbers do not account for bits of the SPI that are used to represent BAK_ID). Now, rather than the SPI_SK identifying only the BAK, the SPI_SK must also contain information to identify the RAND. To implement the RAND value, the SPI_SK is formulated in three parts: 1) the BAK_ID to identify the BAK value to use; 2) the RAND_ID to identify the RAND value to use; and 3) the SPI_RAND value to provide the frequently changing randomness in the SPI_SK.

[1117] FIG. 12A illustrates an SPI_SK 800 portion of an IP packet, including an SPI_RAND 802, a BAK_ID 804, and a RAND_ID 806. The SPI_RAND 802 and BAK_ID 804 are as described hereinabove. To maintain the SPI_SK to a predetermined or specified bit length, the SPI_RAND 802 may use fewer bits than SPI_RAND 612 as in FIG. 9B to allow bits for the RAND_ID 806. The RAND_ID 806 corresponds to the RAND value used for calculation of the SK, and may be a four bit tag or other identifier. The RAND_ID(s) and corresponding RAND value(s) are stored in a LUT at the receiver. FIG. 12B illustrates a RAND LUT 820. The RAND LUT 820 includes an entry for each RAND value listing the RAND_ID and expiration associated with the RAND value.

[1118] FIG. 13 illustrates operation of the CS. For each IP packet, the transmitter determines the BAK that will be used to derive SK, and determines the BAK_ID corresponding to the BAK at step 902. The BAK_ID may be any type of identifier that allows discrimination among multiple BAK values. The CS sends BAK and the BAK_ID to individual users by performing subscription at step 904. The users may perform subscription at various times before and during the subscription period. Steps 902 and 904 may occur before the subscription period starts. At step 906 the transmitter selects a RAND value and determines the corresponding RAND_ID. The CS may send RAND and RAND_ID to the MS individually or send RAND and RAND_ID to be broadcast on the broadcast channel. The value of RAND does not need to be secret, so it is not encrypted. If RAND and RAND_ID are broadcast, then there should not be much time between re-transmission so that an MS does not need to wait long before obtaining the RAND value. Broadcasting RAND and RAND_ID will use a large amount of bandwidth over time. However, if there are a large number of users tuned to the channel, then a large amount of bandwidth will be required to send RAND to each user individually. Consequently, RAND and RAND_ID should only be broadcast if there are a large number of users tuned to the channel. At step 910 the CS chooses a random value of SPI_RAND.

[1119] Once the SPI_RAND, BAK_ID and RAND_ID are known, the transmitter combines them (e.g., concatenates RAND_ID and BAK_ID to the SPI_RAND) to form the SPI_SK at step 912. The CS uses a cryptographic function to combine SPI_RAND, BAK (identified by BAK_ID) and RAND (identified by RAND_ID) to form SK. The CS then encrypts the broadcast message or portion of the message with SK at step 916, and transmits the encrypted message at step 918. Note that the encrypted broadcast message is part of an IP packet that includes the IP header and the ESP header. The ESP header includes the SPI_SK. At decision diamond 920, the CS decides whether to change SK. If the CS decides not to change SK, then the CS proceeds to step 916. If the CS decides to change SK, then the CS proceeds to decision diamond 922, where the CS decides whether to change RAND. If the CS decides not to change RAND, then the CS proceeds to step 910. If the CS decides to change RAND, then the CS proceeds to decision diamond 924,

where the CS decides whether to change BAK. If the CS decides not to change BAK, then the CS proceeds to step 906. If the CS decides to change BAK, then the CS returns to step 902.

[1120] FIG. 14 illustrates the corresponding operation at the receiver, such as a MS. The method 950 initiates when the receiver receives the IP packet including the SPI_SK in the ESP header at step 952. Note that the receiver extracts the SPI_SK information from the IP packet. Upon receipt of the SPI_SK, the receiver first checks if the SK corresponding to the received SPI_SK value is stored in memory at decision diamond 952. In one embodiment, the SPI_SK is stored in an SK LUT is stored in the ME unit 306 of FIG. 4, and in another embodiment, the SPI_SK is stored in the security association database: both of these tables are denoted in FIG. 14 as the SPI table. The check of the SK LUT is performed at decision diamond 954. If the SK value is stored in memory at the receiver, the receiver is able to decrypt the payload of the content packet using the stored SK value at step 956. If the receiver does not have the SK value stored in memory, the receiver extracts BAK_ID and SPI_RAND from SPI_SK at step 958. At step 960, the receiver then checks if the BAK LUT has a valid BAK entry corresponding to BAK_ID. If the BAK LUT does have a valid RAND corresponding to BAK_ID, then the receiver selects this value and proceeds to step 964. If the BAK LUT does not have a valid BAK corresponding to BAK_ID, then (provided the user wishes to subscribe for this period) the receiver performs a subscription to obtain the valid BAK as shown in step 962. The new BAK is stored with BAK_ID in the BAK_LUT and receiver proceeds to step 864. At step 964, the receiver then checks if the RAND LUT has a valid RAND entry corresponding to RAND_ID. If the RAND LUT does have a valid BAK corresponding to RAND_ID, then the receiver selects this value and proceeds to step 964. If the RAND LUT does not have a valid RAND corresponding to RAND_ID, then the receiver obtains RAND and RAND_ID either by requesting the value from the CS or from the broadcast as shown in step 966. The new RAND is stored with RAND_ID in the RAND_LUT and the receiver proceeds to step 968. The receiver combines the BAK corresponding to the BAK_ID value (i.e., BAK_ID in the received SPI_SK), the RAND corresponding to the RAND_ID (i.e., RAND_ID in the received

SPI_SK) and the SPI_RAND value (also in the received SPI_SK) to compute the new SK at step 968. The receiver then uses the new SK value to decrypt the payload of the content packet at step 970. The receiver also stores this SK value indexed by the corresponding SPI_SK and possibly the destination address of the IPSec packets.

[1121] The RAND is changed less frequently than SPI_RAND. The RAND value is common to all mobile stations listening to the broadcast. Therefore, the RAND value may be broadcast to all mobile stations and is not necessarily encrypted specifically per receiver. Therefore, if there are enough mobile stations listening to the broadcast stream, it is more efficient for the air interface to broadcast the RAND value a few times to all these mobile stations rather than require each mobile station to individually request the RAND values from the CS.

[1122] According to one embodiment, the SK calculation is given as:

$$SK=f(SPI\_SK, BAK, RAND), \quad (15)$$

wherein the function is defined as encryption of the SPI_SK using the BAK. As the SPI_SK is made up of the SPI_RAND, the BAK_ID, and the RAND_ID, Equation (15) may also be given as:

$$SK=f(SPI\_RAND, BAK\_ID, RAND\_ID, RAND). \quad (16)$$

[1123] Note that the use of a RAND value may introduce some "blackout periods" because the receiver needs to receive the RAND value on a change. However, these periods are less frequent than when the SK is updated on a separate stream and the receiver waits for the periodic updates. The RAND is designed to change more slowly than the SK value, and therefore, the updates to the RAND are not sent as frequently. The CS would also like to reduce the probability of a "blackout" resulting when an MS stops listening to the channel due to a lost signal, tuning to another channel, or responding to an interruption, such as a phone call. The blackout is most likely to occur at the beginning of the lifetime of a RAND value. To counter this, the CS may re-broadcast the new RAND more frequently around the time when the new RAND value becomes valid. At the end of the lifetime of a RAND, it may become necessary to broadcast both the value of the current RAND and the value of the next RAND.

The values of RAND should not be predictable, and the CS should begin sending RAND only a short time before RAND becomes valid.

[1124] As discussed hereinabove, according to the third exemplary embodiment, SK is derived from BAK, system time and a broadcast random value denoted SK_RAND. FIG. 7C illustrates a method of updating keys for security encryption in a wireless communication system supporting broadcast service. The method 440 implements time periods as given in FIG. 7E. The BAK is updated periodically having a time period T1. A timer t1 is initiated when BAK is calculated and times out at T1. A variable is used for calculating the SK referred to as SK_RAND, which is updated periodically having a time period T2. A timer t2 is initiated when the SK_RAND is generated and times out at T2. In one embodiment, the SK is further updated periodically having a period of T3. A timer t3 is initiated when each SK is generated and time out at time T3. The SK_RAND is generated at the CS and provided periodically to the MS. The MS and the CS use SK_RAND to generate the SK, as detailed hereinbelow.

[1125] A first timer t1 is reset when the applicable value of BAK is updated. The length of time between two BAK updates is the BAK update period. In the exemplary embodiment the BAK update period is a month, however, alternate embodiments may implement any time period desired for optimum operation of the system, or to satisfy a variety of system criteria.

[1126] Continuing with FIG. 7C, the method 440 initializes the timer t2 at step 442 to start the SK_REG time period T2. The CS generates SK_RAND and provides the value to transmit circuitry for transmission throughout the system at step 444. The timer t3 is initialized at step 446 to start the SK time period T3. The CS then encrypts the BC using the current SK at step 448. The encrypted product is the EBC, wherein the CS provides the EBC to transmit circuitry for transmission in the system. If the timer t2 has expired at decision diamond 450, processing returns to step 442. While t2 is less than T2, if the timer t3 has expired at decision diamond 452, processing returns to step 446, else processing returns to 450.

[1127] FIG. 7D illustrates the operation of the MS accessing a broadcast service. The method 460 first synchronizes the timers t2 and t3 with the values at the CS at step 462. The UIM of the MS receives the SK_RAND generated by

the CS at step 464. At step 466 the UIM generates the SK using the SK_RAND, BAK, and a time measurement. The UIM passes the SK to the ME of the MS. The UIM then decrypts the received EBC using the SK to extract the original BC at step 468. When the timer t2 expires at step 470 processing returns to step 462. While the timer t2 is less than T2, if the timer t3 expires at step 472, the timer t3 is initialized at step 474 and returns to 466.

[1128] Key management and updates are illustrated in FIG. 8C, wherein the CS applies a function 508 to generate a value of SK_RAND, which is an interim value used by the CS and MS to calculate SK. Specifically, the function 508 applies the BAK value, the SK_RAND and a time factor. While the embodiment illustrated in FIG. 8C applies a timer to determine when to update the SK, alternate embodiments may use alternate measures to provide periodic updates, for example occurrence of an error or other event. The CS provides the SK_RAND value to each of the subscribers, wherein a function 518 resident in each UIM applies the same function as in function 508 of the CS. The function 518 operates on the SK_RAND, BAK and a timer value to generate a SK that is stored in a memory location in the ME, such as MEM_1 542 of ME_1 540.

[1129] As discussed hereinabove, according to the fourth exemplary embodiment, SK is encrypted using BAK to form SKI, and SKI is sent to the MS. In one exemplary embodiment, SK is sent in an IPSec packet encrypted using BAK. The CS may also broadcast a corresponding SPI that can be used to identify data that is encrypted using SK. This embodiment does not need to be discussed in any more detail.

[1130] In the exemplary embodiments provided hereinabove, the CS may choose to update SK as the CS desires. The more often the SK changes, the more the CS can dissuade attackers from distributing SK values. There will be times when an attacker considers the benefit of distributing SK values to be better than at other times. This will be primarily due to the nature of the content being broadcast. For example, on occurrence of an important event, un-subscribed users will be more interested in receiving news on HSBS, and therefore, will be willing to pay more for illegitimate access than at other times. At these times, the CS may increase the cost and inconvenience to the attacker

and un-subscribed users by changing SK more often than normal. The CS must keep in mind, however, the limits to the processing power of the UIM. If the CS changes SK too often, then the UIM will be unable to compute the SK values in real time, so the users will be unable to decrypt the content in real-time.

[1131] Those of skill in the art would understand that information and signals may be represented using any of a variety of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[1132] Those of skill would further appreciate that the various illustrative logical blocks, modules, circuits, and algorithm steps described in connection with the embodiments disclosed herein may be implemented as electronic hardware, computer software, or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present invention.

[1133] The various illustrative logical blocks, modules, and circuits described in connection with the embodiments disclosed herein may be implemented or performed with a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, or any combination thereof designed to perform the functions described herein. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also

be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[1134] The steps of a method or algorithm described in connection with the embodiments disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module may reside in RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, hard disk, a removable disk, a CD-ROM, or any other form of storage medium known in the art. An exemplary storage medium is coupled to the processor such the processor can read information from, and write information to, the storage medium. In the alternative, the storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in a user terminal. In the alternative, the processor and the storage medium may reside as discrete components in a user terminal.

[1135] The previous description of the disclosed embodiments is provided to enable any person skilled in the art to make or use the present invention. Various modifications to these embodiments will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other embodiments without departing from the spirit or scope of the invention. Thus, the present invention is not intended to be limited to the embodiments shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

[1136] WHAT IS CLAIMED IS:

CLAIMS

1. A method for secure transmissions, the method comprising:
determining a short term key for a message for transmission, the short term key having a short term key identifier;
determining an access key for the message, the access key having an access key identifier;
encrypting the message with the access key;
forming an Internet protocol header comprising the short term key identifier; and
transmitting the encrypted message with the Internet protocol header.

2. The method as in claim 1, wherein the short term key identifier comprises the access key identifier.

3. The method as in claim 2, wherein short term key identifier further comprises a security parameter index value.

4. The method as in claim 3, wherein the security parameter index value is a random number.

5. The method as in claim 1, wherein the short term key is calculated as a function of the short term key identifier and the access key.

6. The method as in claim 5, wherein the short term key identifier is calculated by encrypting the short term key identifier with the access key.

7. The method as in claim 1, wherein the Internet protocol header is part of an ESP header.

8. The method as in claim 7, wherein the Internet protocol header further comprises a second random number, the second random number having a random number identifier.

9. The method as in claim 8, wherein the short term key identifier comprises the access key identifier and the random number identifier.

10. The method as in claim 9, wherein short term key identifier further comprises a security parameter index value.

11. The method as in claim 10, wherein the security parameter index value is a random number.

12. The method as in claim 8, wherein the short term key is calculated as a function of the short term key identifier, the second random number, and the access key.

13. The method as in claim 12, wherein the short term key identifier is calculated by encrypting the short term key identifier and the second random number with the access key.

14. A method for secure reception of a transmission, the method comprising:
receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key;
determining an access key based on the short term key identifier;
encrypting the short term key identifier with the access key to recover the short term key; and
decrypting the transmission using the short term key.

15. The method as in claim 14, further comprising:
storing the short term key identifier and short term key in a memory storage unit.

16. The method as in claim 14, wherein the short term key identifier is comprised of a random number and an access key identifier associated with the access key.

17. The method as in claim 14, wherein encrypting the short term key identifier further comprises encrypting the short term key identifier and a random number with the access key to recover the short term key.

18. In a wireless communication system supporting a broadcast service option, an infrastructure element comprising:

a receive circuitry;

a user identification unit, operative to recover a short-time key for decrypting a broadcast message, comprising:

processing unit operative to decrypt key information; and

a mobile equipment unit adapted to apply the short-time key for decrypting the broadcast message, comprising:

memory storage unit for storing a plurality of short term keys and short term key identifiers.

19. The infrastructure element as in claim 15, wherein the user identification unit further comprises a second memory storage unit for storing a plurality of access keys and access key identifiers.

20. The infrastructure element as in claim 15, wherein the memory storage unit is a secure memory storage unit.

21. An infrastructure element for a wireless communication system, comprising:

means for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key;

means for determining an access key based on the short term key identifier;

means for encrypting the short term key identifier with the access key to recover the short term key; and

means for decrypting the transmission using the short term key.

22. A digital signal storage device, comprising:

first set of instructions for receiving a short term key identifier specific to a transmission, the short term key identifier corresponding to a short term key;

second set of instructions for determining an access key based on the short term key identifier;

third set of instructions for encrypting the short term key identifier with the access key to recover the short term key; and

fourth set of instructions for decrypting the transmission using the short term key.

23. A communication signal transmitted on a carrier wave, comprising:

a first portion corresponding to a short term key identifier, the short term key identifier having a corresponding short term key; and

a second portion corresponding to a transmission payload encrypted using the short term key.

24. The communication signal as in claim 23, wherein the short term key identifier comprises:

a random number portion; and

an access key identifier corresponding to an access key.

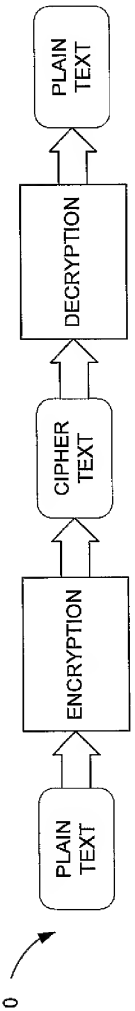


FIG. 1A

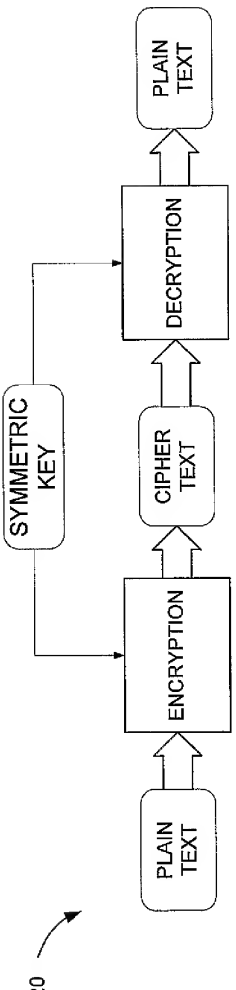


FIG. 1B

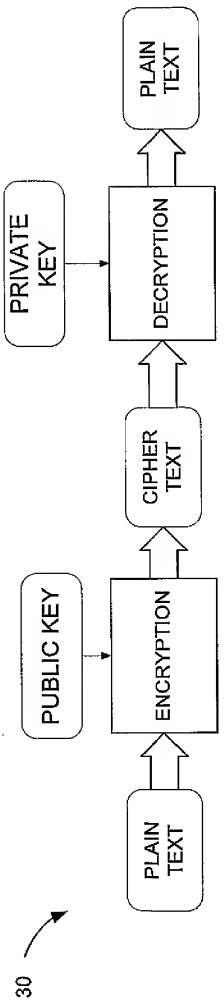


FIG. 1C

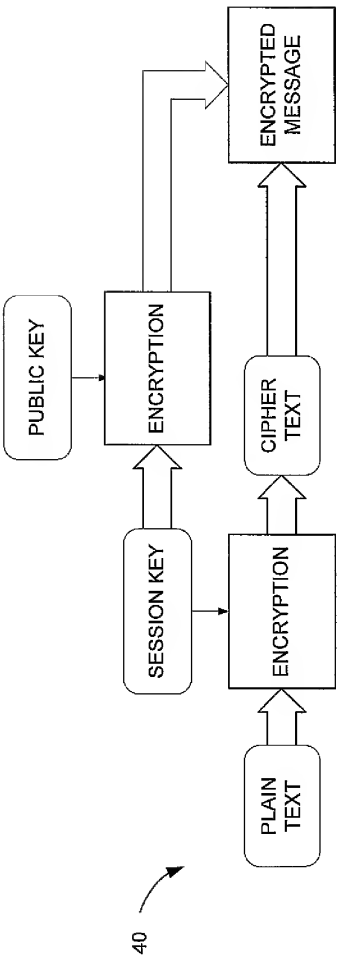

ENCRYPTED MESSAGE
PUBLIC KEY
ENCRYPTION
CIPHER TEXT
SESSION KEY
ENCRYPTION
PLAIN TEXT
40

FIG. 1D

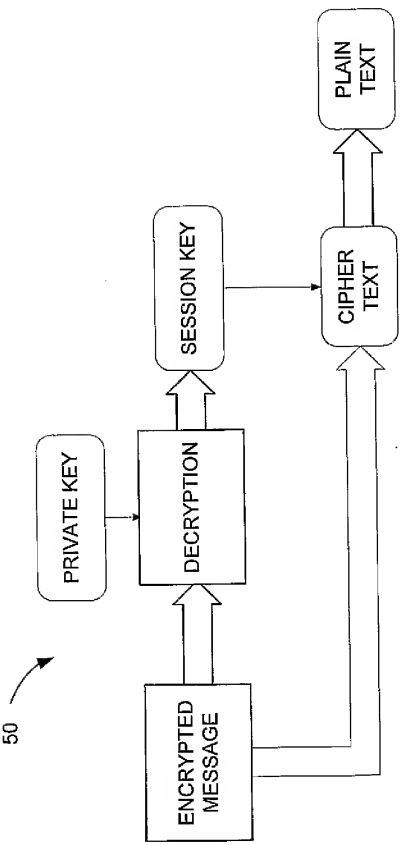

50
ENCRYPTED MESSAGE
PRIVATE KEY
DECRYPTION
SESSION KEY
CIPHER TEXT
PLAIN TEXT

FIG. 1E

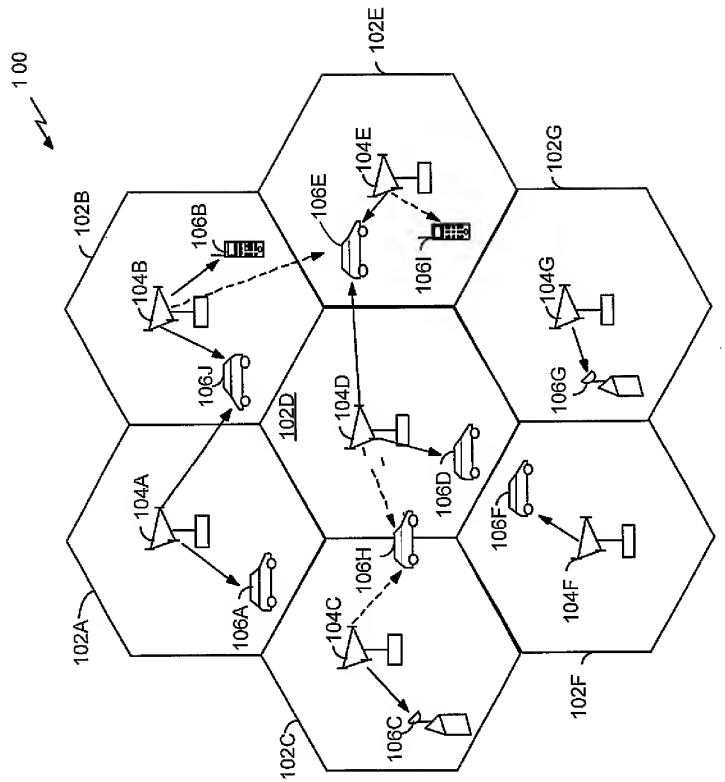

100
102A
102B
102C
102D
102E
102F
102G
104A
104B
104C
104D
104E
104F
104G
106A
106B
106C
106D
106E
106F
106G
106H
106I
106J

FIG. 2

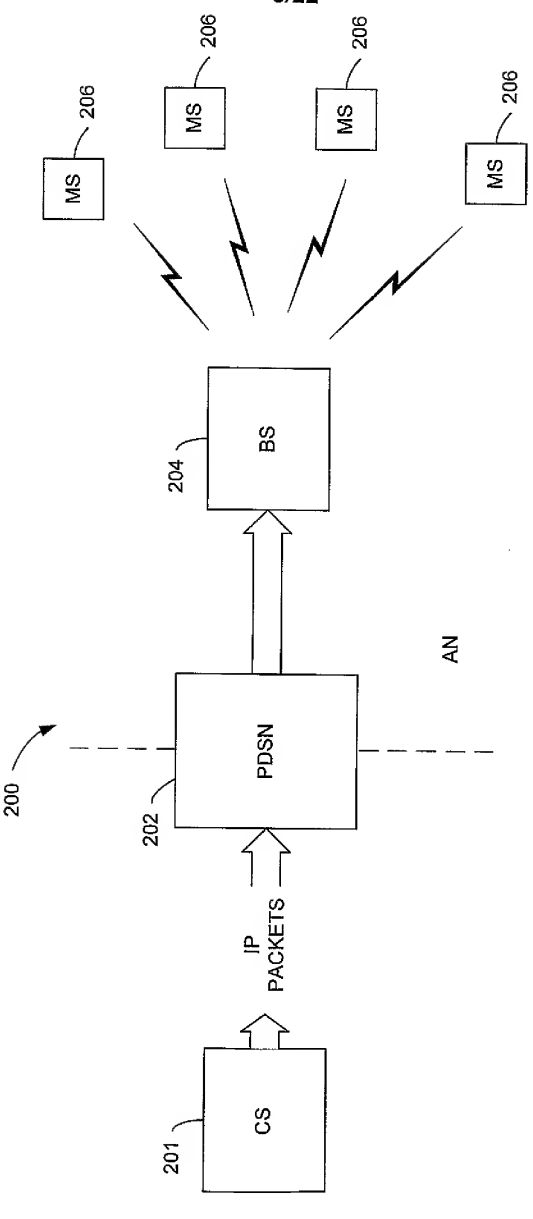

MS
206
MS
206
MS
206
MS
206
BS
204
AN
PDSN
202
200
IP
PACKETS
CS
201

FIG. 3

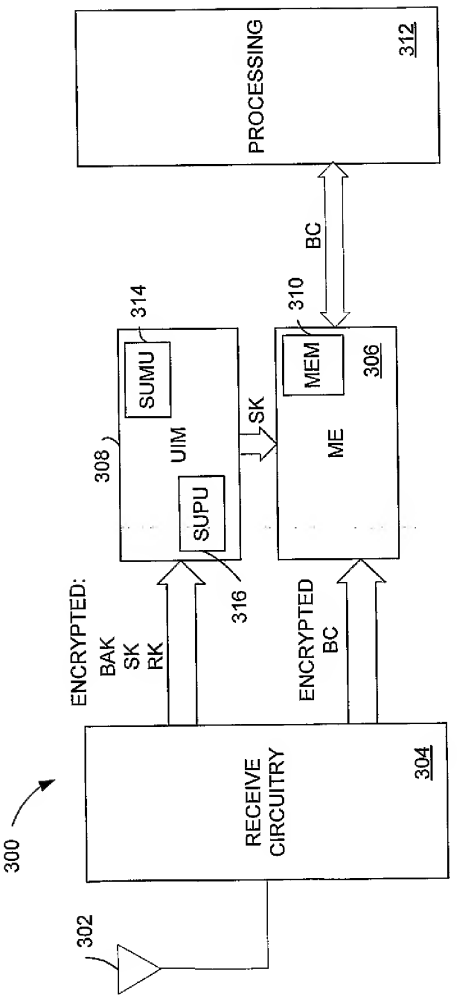

PROCESSING
312
BC
314
310
SUMU
MEM
306
308
UIM
SK
ME
SUPU
316
ENCRYPTED:
BAK
SK
RK
ENCRYPTED
BC
RECEIVE
CIRCUITRY
304
300
302

FIG. 4

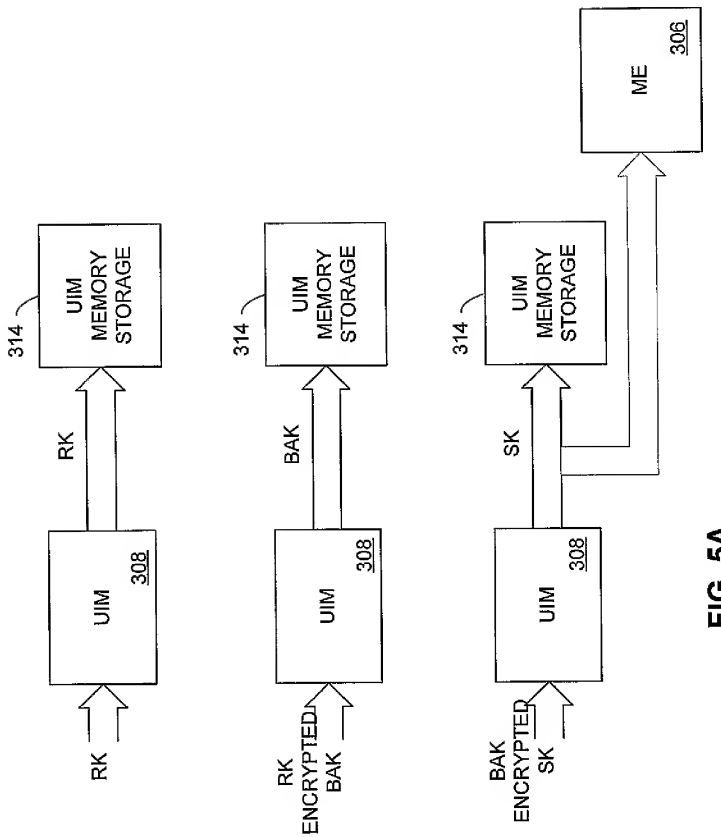

RK
UIM 308
RK
314
UIM MEMORY STORAGE
RK ENCRYPTED BAK
UIM 308
BAK
314
UIM MEMORY STORAGE
BAK ENCRYPTED SK
UIM 308
SK
314
UIM MEMORY STORAGE
ME 306

FIG. 5A

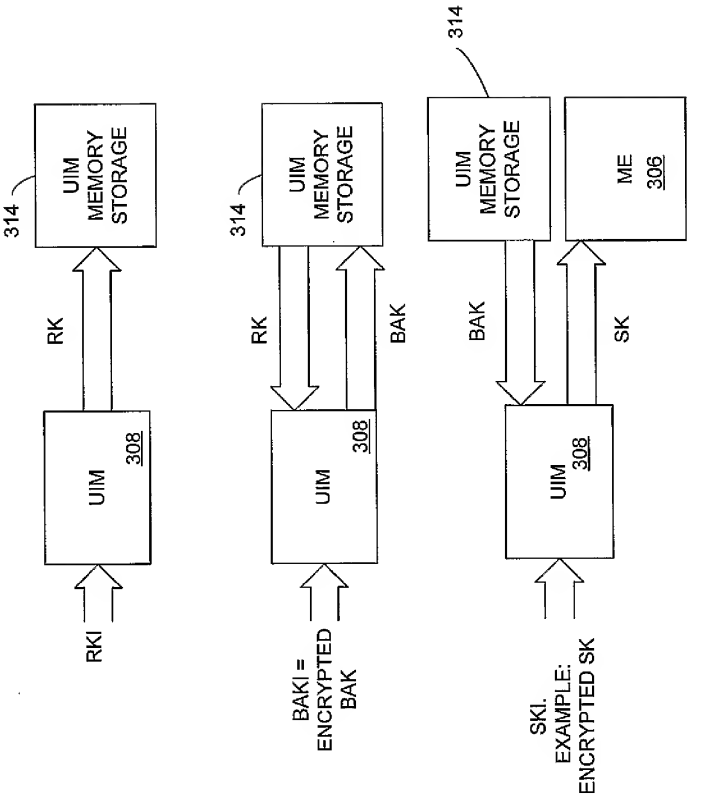

314
UIM MEMORY STORAGE
RK
UIM 308
RKI
314
UIM MEMORY STORAGE
RK
BAK
UIM 308
BAKI = ENCRYPTED BAK
314
UIM MEMORY STORAGE
ME 306
BAK
SK
UIM 308
SKI. EXAMPLE: ENCRYPTED SK

FIG. 5B

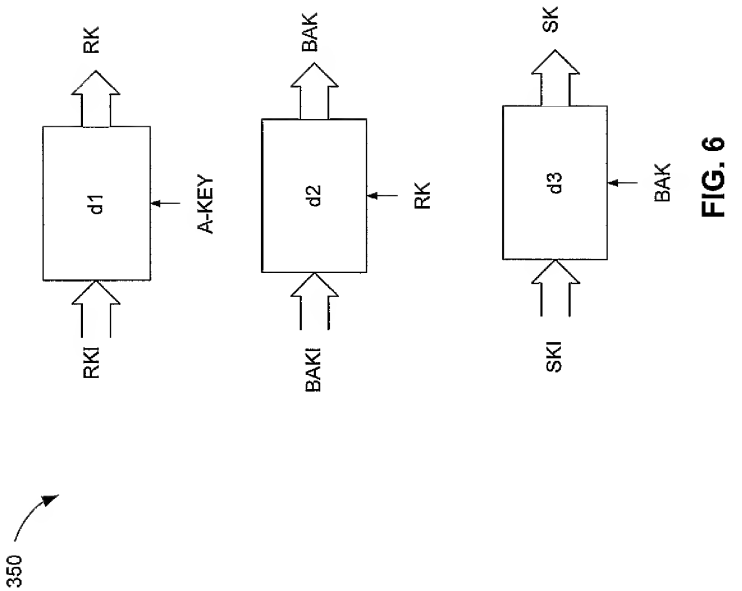


FIG. 6

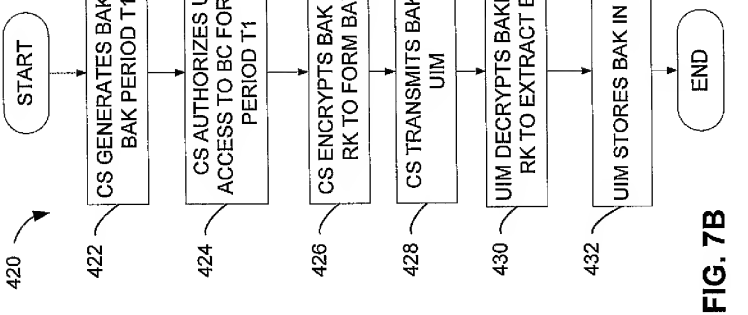

420
START
422
CS GENERATES BAK FOR BAK PERIOD T1
424
CS AUTHORIZES UIM ACCESS TO BC FOR BAK PERIOD T1
426
CS ENCRYPTS BAK WITH RK TO FORM BAKI
428
CS TRANSMITS BAKI TO UIM
430
UIM DECRYPTS BAKI WITH RK TO EXTRACT BAK
432
UIM STORES BAK IN SUMU
END

FIG. 7B

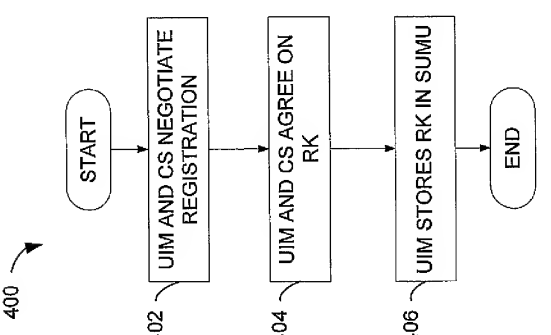

400
START
402
UIM AND CS NEGOTIATE REGISTRATION
404
UIM AND CS AGREE ON RK
406
UIM STORES RK IN SUMU
END

FIG. 7A

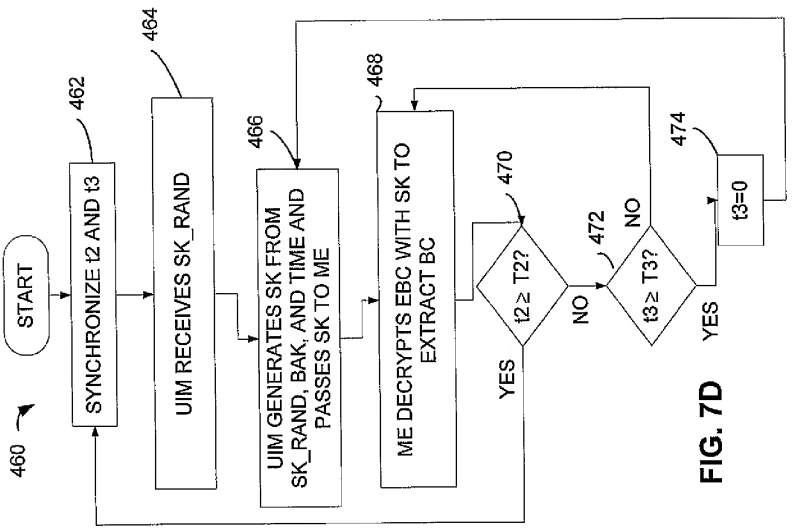

460
START
462
SYNCHRONIZE t2 AND t3
464
UIM RECEIVES SK_RAND
466
UIM GENERATES SK FROM SK_RAND, BAK, AND TIME AND PASSES SK TO ME
468
ME DECRYPTS EBC WITH SK TO EXTRACT BC
470
t2≥ T2?
YES
NO
472
t3≥ T3?
NO
YES
474
t3=0

FIG. 7D

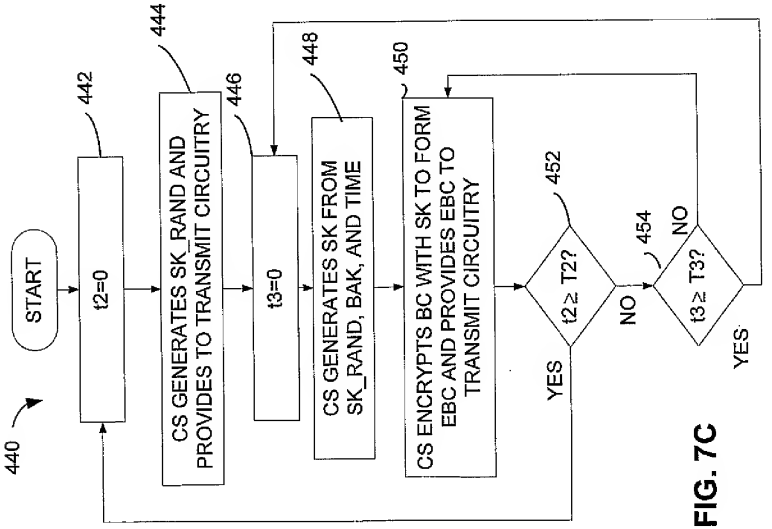

440
START
442
t2=0
444
CS GENERATES SK_RAND AND PROVIDES TO TRANSMIT CIRCUITRY
446
t3=0
448
CS GENERATES SK FROM SK_RAND, BAK, AND TIME
450
CS ENCRYPTS BC WITH SK TO FORM EBC AND PROVIDES EBC TO TRANSMIT CIRCUITRY
452
t2≥ T2?
YES
NO
454
t3≥ T3?
NO
YES

FIG. 7C

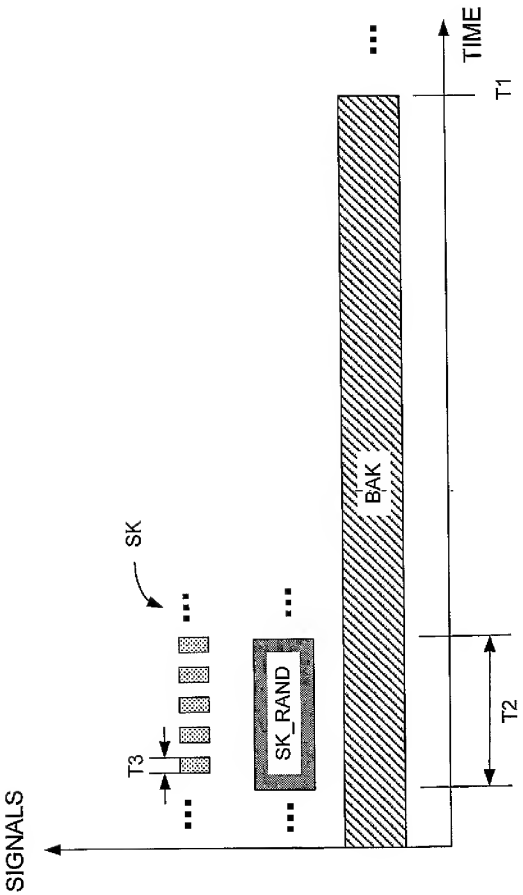


FIG. 7E

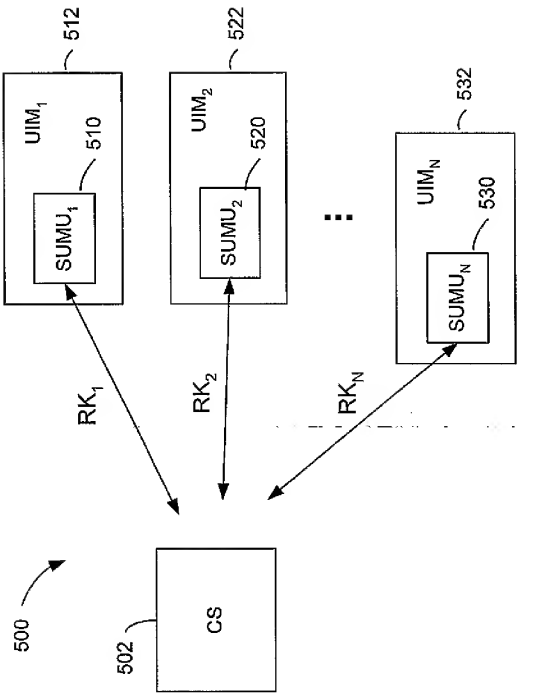

512
UIM1
510
SUMU1
522
UIM2
520
SUMU2
532
UIMN
530
SUMUN
RK1
RK2
RKN
500
502
CS

FIG. 8A

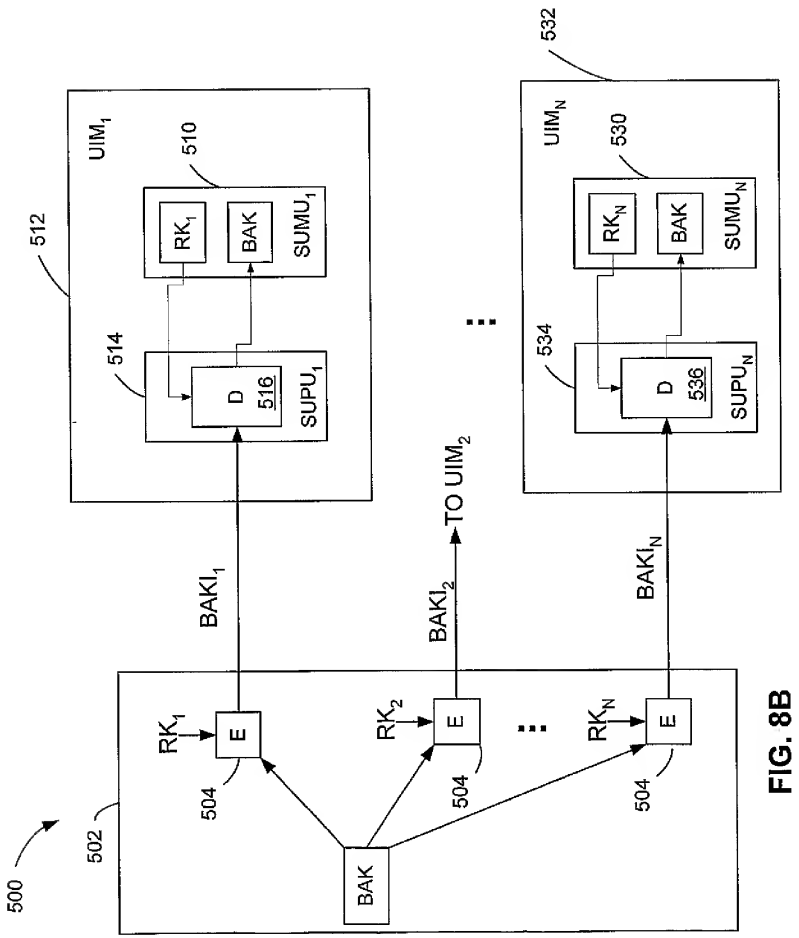

500
502
BAK
RK1
E
504
RK2
E
504
RKN
E
504
BAKI1
BAKI2
TO UIM2
BAKIN
UIM1
512
510
RK1
BAK
SUMU1
514
D
516
SUPU1
UIMN
532
530
RKN
BAK
SUMUN
534
D
536
SUPUN

FIG. 8B

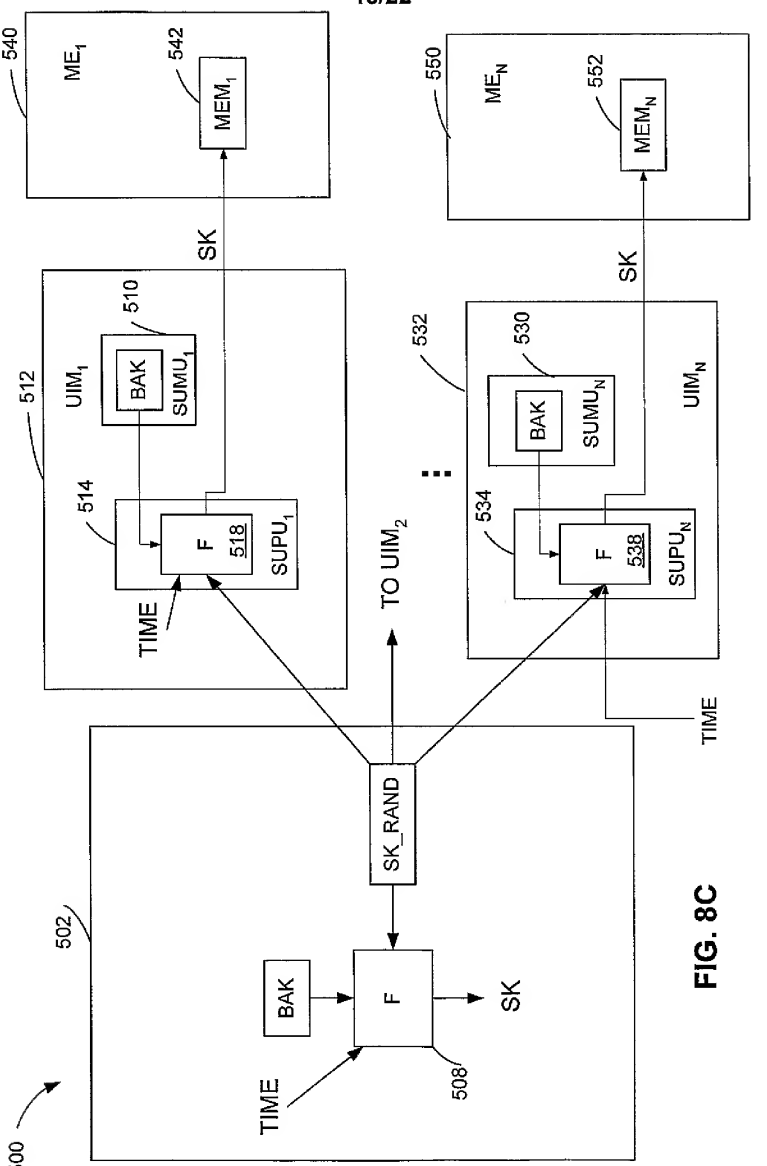

500
502
BAK
F
SK
TIME
508
SK_RAND
TO UIM2
TIME
512
UIM1
510
BAK
SUMU1
514
F
518
SUPU1
TIME
SK
540
ME1
542
MEM1
532
UIMN
530
BAK
SUMUN
534
F
538
SUPUN
SK
550
MEN
552
MEMN

FIG. 8C

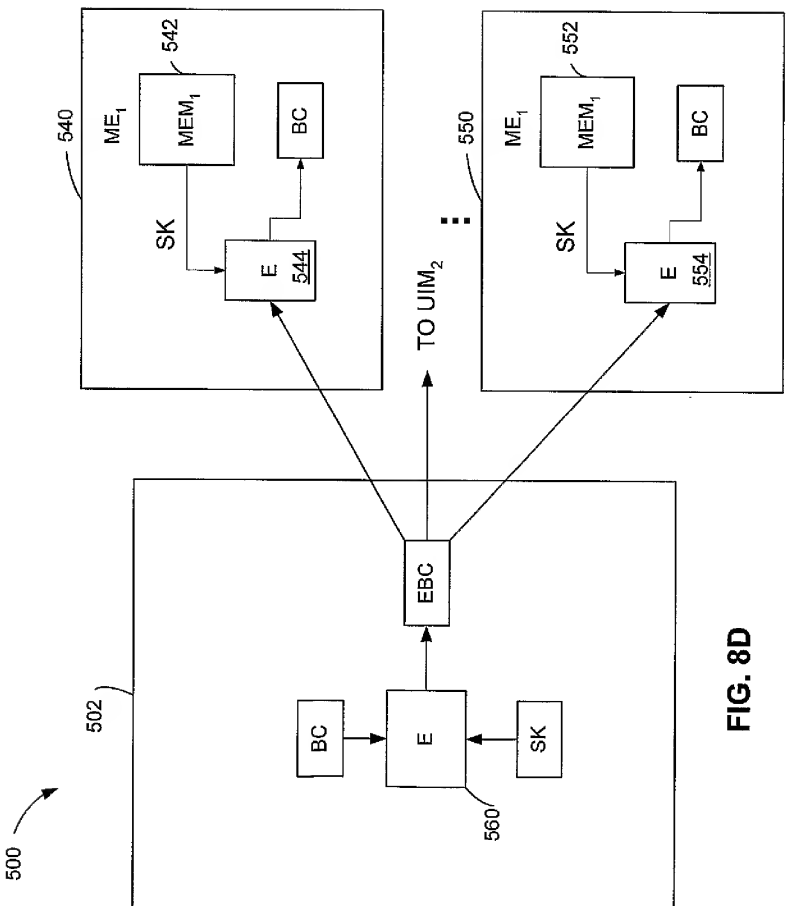

500
502
BC
E
SK
560
EBC
TO UIM2
540
ME1
MEM1
542
SK
E
544
BC
550
ME1
MEM1
552
SK
E
554
BC

FIG. 8D

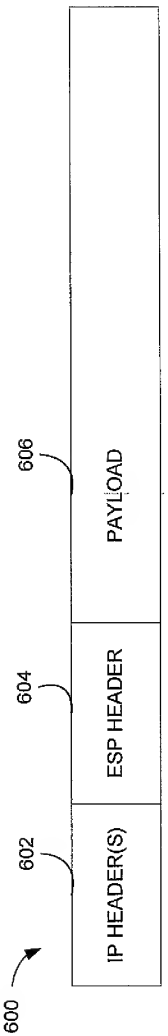

600
602
IP HEADER(S)
604
ESP HEADER
606
PAYLOAD

FIG. 9A

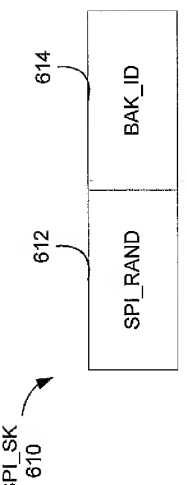

SPI_SK
610
612
SPI_RAND
614
BAK_ID

FIG. 9B

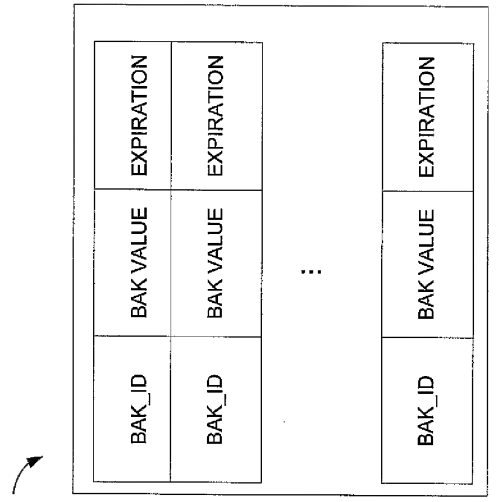

630
BAK_ID
BAK VALUE
EXPIRATION
BAK_ID
BAK VALUE
EXPIRATION
BAK_ID
BAK VALUE
EXPIRATION

FIG. 9D

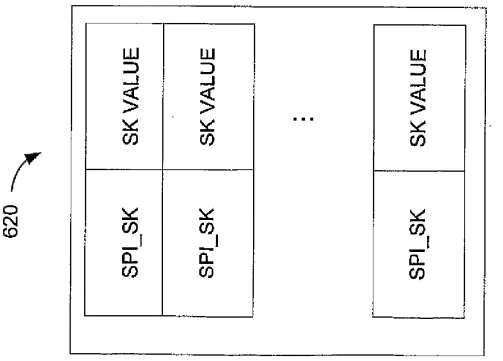

620
SPI_SK
SK VALUE
SPI_SK
SK VALUE
SPI_SK
SK VALUE

FIG. 9C

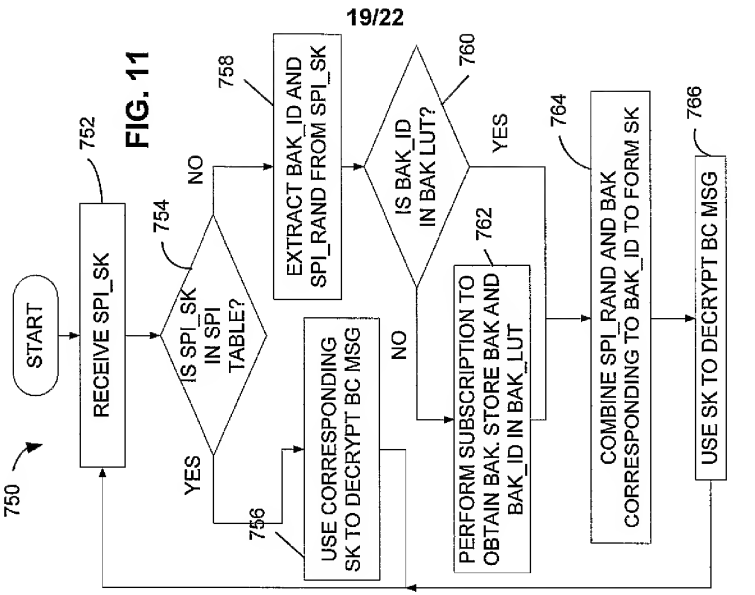

750
START
RECEIVE SPI_SK
752
IS SPI_SK IN SPI TABLE?
754
YES
NO
756
USE CORRESPONDING SK TO DECRYPT BC MSG
EXTRACT BAK_ID AND SPI_RAND FROM SPI_SK
758
IS BAK_ID IN BAK LUT?
760
NO
YES
PERFORM SUBSCRIPTION TO OBTAIN BAK. STORE BAK AND BAK_ID IN BAK_LUT
762
COMBINE SPI_RAND AND BAK CORRESPONDING TO BAK_ID TO FORM SK
764
USE SK TO DECRYPT BC MSG
766

FIG. 11

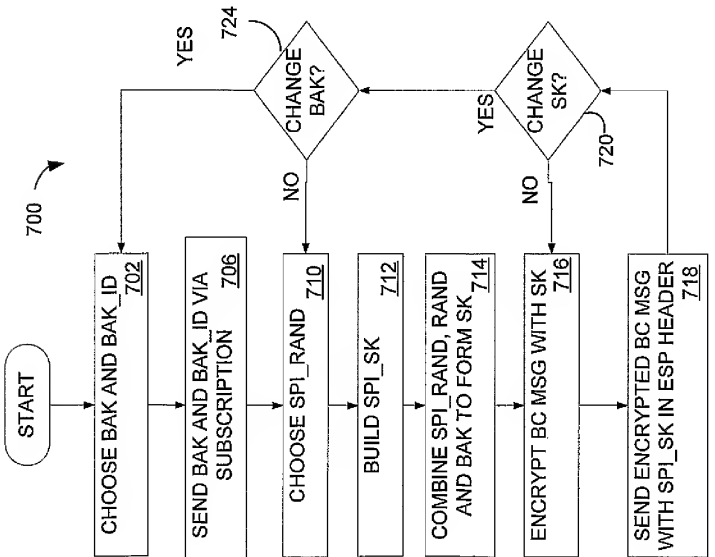

700
START
CHOOSE BAK AND BAK_ID
702
SEND BAK AND BAK_ID VIA SUBSCRIPTION
706
CHOOSE SPI_RAND
710
BUILD SPI_SK
712
COMBINE SPI_RAND, RAND AND BAK TO FORM SK
714
ENCRYPT BC MSG WITH SK
716
SEND ENCRYPTED BC MSG WITH SPI_SK IN ESP HEADER
718
CHANGE BAK?
724
YES
NO
CHANGE SK?
720
YES
NO

FIG. 10

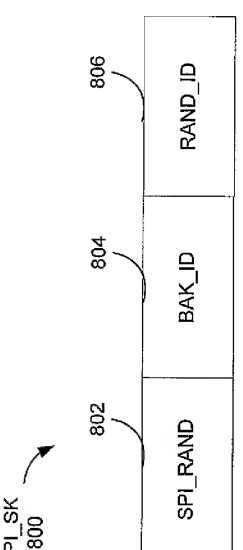


FIG. 12A

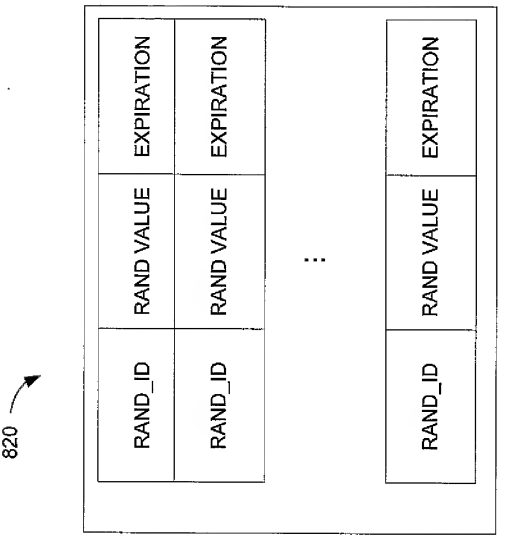


FIG. 12B

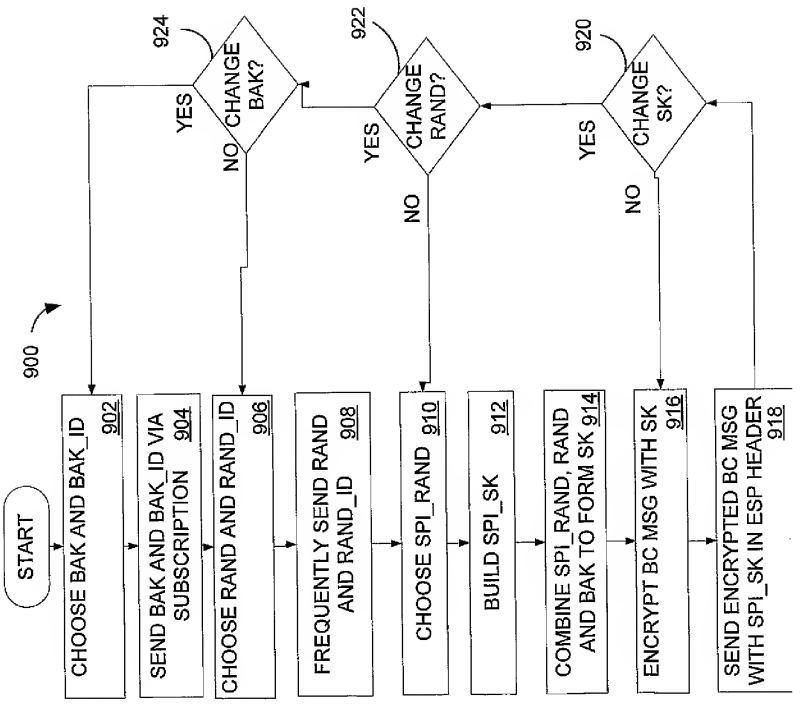

900
START
CHOOSE BAK AND BAK_ID 902
SEND BAK AND BAK_ID VIA SUBSCRIPTION 904
CHOOSE RAND AND RAND_ID 906
FREQUENTLY SEND RAND AND RAND_ID 908
CHOOSE SPI_RAND 910
BUILD SPI_SK 912
COMBINE SPI_RAND, RAND AND BAK TO FORM SK 914
ENCRYPT BC MSG WITH SK 916
SEND ENCRYPTED BC MSG WITH SPI_SK IN ESP HEADER 918
924
CHANGE BAK?
YES
NO
922
CHANGE RAND?
YES
NO
920
CHANGE SK?
YES
NO

FIG. 13

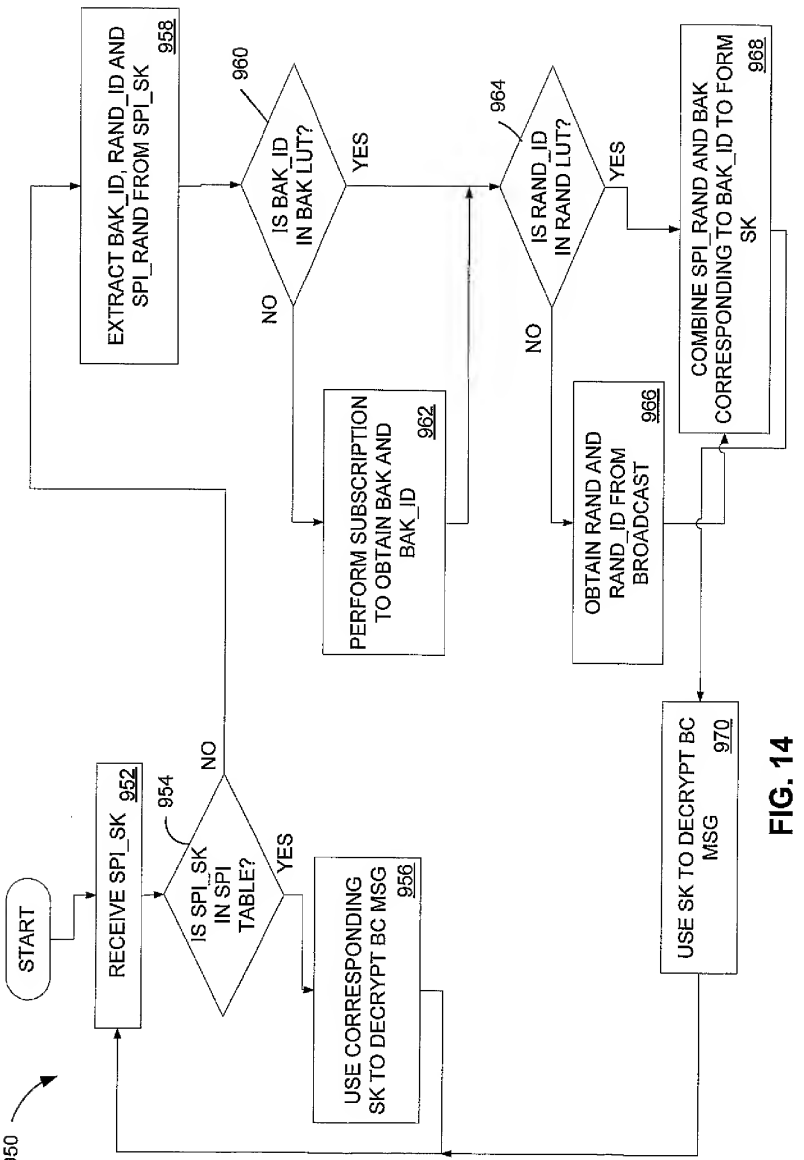

950
START
RECEIVE SPI_SK 952
954
IS SPI_SK IN SPI TABLE?
NO
YES
USE CORRESPONDING SK TO DECRYPT BC MSG 956
EXTRACT BAK_ID, RAND_ID AND SPI_RAND FROM SPI_SK 958
960
IS BAK_ID IN BAK LUT?
NO
YES
PERFORM SUBSCRIPTION TO OBTAIN BAK AND BAK_ID 962
964
IS RAND_ID IN RAND LUT?
NO
YES
OBTAIN RAND AND RAND_ID FROM BROADCAST 966
COMBINE SPI_RAND AND BAK CORRESPONDING TO BAK_ID TO FORM SK 968
USE SK TO DECRYPT BC MSG 970

FIG. 14

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 April 2003 (17.04.2003)

PCT

(10) International Publication Number
WO 03/032573 A3

(51) International Patent Classification[7]: H04L 9/08, 29/06

(21) International Application Number: PCT/US02/32054

(22) International Filing Date: 8 October 2002 (08.10.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/973,301 9 October 2001 (09.10.2001) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121 (US).

(72) Inventors: HAWKES, Philip; 2/6-8 Belmore Street, Burwood, New South Wales 2134 (AU). LEUNG, Nikolai K., N.; 7710 Takoma Avenue, Takoma Park, MD 20912 (US). ROSE, Gregory G.; 6 Kingston Avenue, Mortlake, New South Wales 2137 (AU).

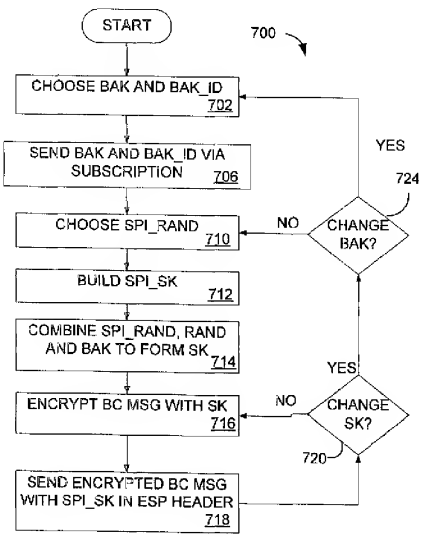
(74) Agents: WADSWORTH, Philip, R. et al.; QUALCOMM Incorporated, 5775 Morehouse Drive, San Diego, CA 92121 (US).

(81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURITY IN A DATA PROCESSING SYSTEM



(57) Abstract: Method and apparatus for secure transmissions. Each user is provided a registration key. A long-time updated broadcast key is encrypted using the registration key and provided periodically to a user. A short-time updatedkey is encrypted using the broadcast key. The short-time key is available with each broadcast message,wherein sufficient information to calculate the short-time key is provided in an Internet protocol headerpreceding the broadcast content. Broadcasts are then encrypted using the short-time key, wherein the user decrypts the broadcast message using the short-time key.

WO 03/032573 A3

Published:
with international search report

(88) Date of publication of the international search report:
30 October 2003

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Internat! Application No
PCT/US 02/32054

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WILLIAN STALLINGS: "Cryptography and network security" 1995 , PRENTICE-HALL, INC. , NEW JERSEY XP002248261 * page 402 - page 406 * * page 413 - page 417 * * page 421 - page 424 *	1-24
A	MENEZES, VANSTONE, OORSCHOT: "Handbook of Applied Cryptography" 1997 , CRC PRESS LLC , USA XP002248262 * page 497 - page 500 * * page 551 - page 552 *	1-24

-/—

[X] Further documents are listed in the continuation of box C.

[ ] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 July 2003	05/08/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	San Millán Maeso, J

2

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	BRUCE SCHNEIER: "Applied Cryptography Second Edition" 1996 , JOHN WILEY & SONS, INC. XP002248263 * page 520 * page 523 -page 524	1-24

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L — A2

(11) International Publication Number: **WO 96/11538**

(43) International Publication Date: 18 April 1996 (18.04.96)

(21) International Application Number: PCT/NL95/00334

(22) International Filing Date: 3 October 1995 (03.10.95)

(30) Priority Data:
9401626 4 October 1994 (04.10.94) NL

(71) Applicant *(for all designated States except US)*: MULTI-HOUSE AUTOMATISERING B.V. [NL/NL]; Doesburgweg 7, NL-2803 PL Gouda (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HARDENDOOD, Theo [NL/NL]; Vredebest 15, NL-2801 AS Gouda (NL).

(74) Agent: 't JONG, Bastiaan, Jacobus; Arnold & Siedsma, Sweelinckplein 1, NL-2517 GK The Hague (NL).

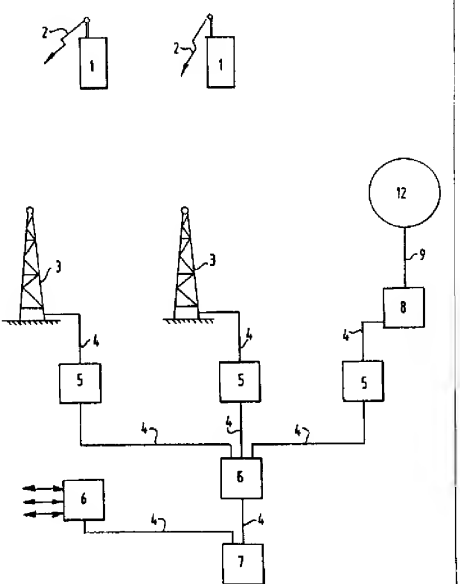
(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: SYSTEM FOR DIGITAL COMMUNICATION

(57) Abstract

The invention relates to a system for digital communication of data divided into packets between at least two communication apparatuses via a network, said network comprising at least two media, wherein communication in the network is controlled by a network protocol and communication between the apparatuses is controlled by an apparatus protocol. Unabbreviated and complete transfer through the network of data and apparatus protocol information supplemented with network protocol information results in unnecessarily bulky packets, since at least some of the functions of the apparatus protocol are likewise executed by the network protocol, wherein the cost of the transfer through the network is directly proportional to the number of packets for transfer and the size of these packets. The invention has for its object to obviate the above stated drawbacks and provides to this end a system which is distinguished in that between the network and at least one of the apparatuses is placed a gate device which is adapted to code or decode the apparatus protocol information contained in a packet together with the data for transfer and to add network protocol information to the packet or remove it therefrom, and the system is further distinguished in that the gate device is adapted to transmit to an apparatus a confirmation to acknowledge receipt of a packet transmitted by this apparatus and to transfer the packet to the network for further transmission to the destination apparatus.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgystan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

SYSTEM FOR DIGITAL COMMUNICATION

The invention relates to a system for digital communication of data divided into packets between at least two communication apparatuses via a network, said network comprising at least two media, wherein communication in the network is controlled by a network protocol and communication between said apparatuses is controlled by an apparatus protocol.

It is known in the art to make use of a system wherein the data to be transferred from apparatus to apparatus and the apparatus protocol information are transferred in full and unabbreviated through the network. For this transfer through the network the packet is simply supplemented with the network protocol information required for this purpose.

TCP/IP and MPAK are for instance the apparatus protocol and network protocol respectively. One of the media of the network is, for example, the ether through which radio links are effected, wherein such a network with digital radio links is for instance the MOBITEX network.

In the case that the network contains a part which is formed by a medium through which transfer of data is only possible at a lesser rate, such as a digital radio network only having available a limited band width, the following problems herein occur.

Unabbreviated and complete transfer through the network of data and apparatus protocol information supplemented with the network protocol information results in unnecessarily bulky packets, since at least some of the functions of the apparatus protocol are likewise executed by the network protocol, wherein the cost of the transfer through the network is directly proportional to the number of packets for transfer and the size of these packets.

The invention has for its object to obviate the above stated drawbacks and provides to this end a system which is distinguished in that between the network and at least one of the apparatuses is placed a gate device which is adapted to code or decode the apparatus protocol information contained in a packet together with the data for transfer and to add network protocol information to the packet or remove it therefrom.

In many known systems the transferring apparatus will expect under the apparatus protocol a confirmation sent within a predetermined time by the receiving apparatus to acknowledge receipt of a transmitted packet, wherein the transferring apparatus will transmit the relevant packet again when such a confirmation is not received within this time. This time duration is however usually geared to transfer of packets between communication apparatuses via a network with high transfer rates, for instance a local area network with fixed cable connections such as the datanet or the internet. Since both the packet and a confirmation to acknowledge receipt thereof are transferred through the slower part of the network at a speed lower than the transfer rate to which the repetition time of the apparatus protocol is geared, such a confirmation will not reach the transferring apparatus in good time to prevent repeated transmission of the relevant packet. The cost of transferring the packets hereby rises unnecessarily and there is the danger of the network becoming overloaded.

In accordance with the above the system is further distinguished in that the gate device is adapted to send to an apparatus a confirmation to acknowledge receipt of a packet transmitted by this apparatus and to transfer the packet to the network for further transmission to the destination apparatus.

A system according to the present invention therefore has the advantage that the size of packets for

transfer is limited and unnecessarily repeated transmission of packets is prevented.

The invention is further elucidated with reference to the figure description of an embodiment of the invention following hereinbelow. In the drawing:

fig. 1 shows a schematic view of a system according to the present invention;

fig. 2 shows a schematic view of a local area network; and

fig. 3 shows a schematic view of a packet to be transferred by the system shown in fig. 1.

The embodiment of the invention shown in fig. 1 comprises: communication apparatuses formed by mobile stations 1 and another communication apparatus 12; a network 13, which network 13 comprises: transmitting and receiving stations 3; fixed cable connections 4; local nodes 5; regional nodes 6; and a central node 7; and a gate device 8 placed between the network 13 and the communication apparatus 12.

The mobile stations 1 are in contact with the transmitting and receiving stations by means of a radio link 3, wherein a limited band width is available for this radio link, which imposes a limitation on the transfer rate between the mobile stations 1 and the transmitting and receiving stations 3.

The transmitting and receiving stations 3 are each connected by means of fixed cable connections to a local node 5. It is noted here, that a local node can be connected to a plurality of transmitting and receiving stations 3. Three local nodes 5 are herein connected to a regional node 6 by means of fixed cable connections 4, wherein in the case shown two nodes 6 are connected in turn to a central node 7 by means of fixed cable connections 4.

An example of such a network with a hierarchical branch structure is the MOBITEX network which is particularly suitable for transferring packets of digital data, which packets together form a message. A

description follows below wherein the message is transferred from a communication apparatus 12 via the network 13 to the mobile station 1.

The communication apparatuses 12 are formed in the embodiment of the invention shown here by storage means for storing and retrieving data, wherein at the request of mobile stations 1 these means transmit requested data from their files to the mobile stations 1 via the network 13.

The making of the connection, retrieval of data from the files of servers, transmitting of the retrieved data etc. is controlled by an apparatus protocol such as the TCP/IP protocol which in practice has become a standard protocol for transfer of packets of digital data between communication apparatuses. Such an apparatus protocol, and in particular the TCP/IP protocol, is however particularly suitable for such a transfer via a network of fixed cable connections, for instance a local area network such as the ethernet or the datanet, wherein due to the high transfer rates problems are caused by a slower medium acting as a bottleneck in the network 13. Transfer in network 13 is therefore controlled by a separate network protocol such as the MPAK protocol.

In contrast to the known art, wherein network protocol information is simply added to the packet consisting of apparatus protocol information and data, a gate device 8 is arranged in the system according to the present invention, wherein a processing unit present in the gate device codes only the necessary apparatus protocol information and removes the rest and subsequently adds the network protocol information. Since correct transfer of packets through the network under the control of the network protocol is already ensured, it is for instance not necessary to also transfer separate information for this purpose in the apparatus protocol information.

Also, immediately after receiving a packet, the gate device sends back a confirmation to acknowledge receipt

to the transmitting communication apparatus 12, which is permitted since correct transfer is already ensured under the network protocol.

In addition, the non-coded apparatus protocol information is transferred through the network once in a first packet together with the key, thus enabling decoding by the mobile station 1 of coded apparatus protocol information in following packets. It is especially notable here that the information regarding the origin and the destination in the apparatus protocol information is coded by gate device 8 to a single session code from which the mobile station 1 can identify and receive a packet transmitted thereafter.

The gate device is further provided with means for compressing the data, thereby realizing a further reduction in the number of packets for transfer and/or the size of the packets for transfer. Use can be made for this purpose of a compression algorithm which is particularly suitable for the mobile station 1 and which is supplied to gate device 8 from a communication apparatus 12, or of a compression algorithm already present in the gate device. In all functions the gate device 8 is transparent for the communication apparatuses so that the latter can operate with the same apparatus protocol irrespective of whether or not the gate device 8 is present.

In the embodiment of the invention shown in fig. 1 another gate device forms a unit with a mobile station 1, wherein this gate device removes the network protocol information and decodes the apparatus protocol information.

According to another embodiment in accordance with the present invention an additional network is situated on the destination side of the radio link 2 instead of the mobile stations 1 shown here. Such a network can take a form similar to the network shown in fig. 1 between the radio link 2 and the fixed cable connection 9.

It is further conceivable that the network 13 contains mutual connections between local nodes 5 and/or mutual connections between the regional nodes 6. When packets forming a message are transferred via such a network the route covered by the packets is not fixed and the sequence of arrival can vary from the sequence in which the packets are transmitted as a result of different "transmission times". It will be apparent that other network configurations can also be applied.

Shown in fig. 2 are: the network 12; cable connection 9; gate device 8; cable connections 10; and communication apparatuses 11a, 11b and 11c.

The communication apparatuses 11a, 11b and 11c are for instance provided with databases, wherein a policeman can for instance retrieve from these nationally accessible databases data relating to the number plates of a car or the personal details of someone who has been detained, or wherein an employee or representative of a company can for instance retrieve from these databases placed on the company premises data relating to stock, delivery times or prices.

A selection device 14 herein provides the connection between the network 13 and one of the communication apparatuses 11a, 11b or 11c via the gate device 8.

Shown schematically in fig. 3 is the format of a packet 20 for transfer, which packet 20 comprises a part A containing protocol information and a part B containing the data for transfer.

In the embodiment shown in fig. 1 and fig. 2 the part A of packet 20 contains a block 21 of network protocol information for the MPAK protocol and two blocks 22, 23 for the apparatus protocol information of respectively the TCP protocol and the IP protocol. The whole part B of packet 20 is taken up by a block 24 with data for transfer.

When a packet 20 is transferred between a communication apparatus 12 and the gate device 8 the packet 20 does not contain a block 21 with the network

protocol information. When a packet 20 is transferred from gate device 8 through the network 13, the block 21 containing information for the MPAK network protocol will have been added, the blocks 22, 23 containing respectively TCP apparatus protocol information and IP apparatus protocol information will have been coded by gate device 8 and the block 24 of packet 20 containing data for transfer will have been compressed by the gate device 8.

CLAIMS

1. System for digital communication of data divided into packets between at least two communication apparatuses via a network, which network comprises at least two media, wherein communication in the network is controlled by a network protocol and communication between the apparatuses is controlled by an apparatus protocol, **characterized in that** between the network and at least one of the apparatuses is placed a gate device which is adapted to code or decode the apparatus protocol information contained in a packet together with the data for transfer and to add network protocol information to the packet or remove it therefrom.

2. System for data communication as claimed in claim 1, **characterized in that** the gate device is adapted to transmit complete coding information once through the network to a memory means in the destination apparatus or in a gate device on the destination side.

3. System for data communication as claimed in claim 1 or 2, **characterized in that** one or more than one apparatus forms a unit with a gate device.

4. System for data communication as claimed in claim 1 or 2, **characterized in that** the gate device is adapted to convert the origin information and the destination information in the apparatus protocol information into a single session code.

5. System for data communication as claimed in claim 1, **characterized in that** the gate device is adapted to send to an apparatus a confirmation of reception of a packet transmitted by this apparatus and to transfer the packet to the network for further transmission to the destination apparatus.

6. System for data communication as claimed in claim 1, **characterized in that** the gate device is adapted to code the data for transfer.

7. System for data communication as claimed in claim 1 or 6, **characterized in that** the gate device is adapted to execute the coding in accordance with a coding algorithm chosen or supplied by a user.

8. System for data communication as claimed in claim 1, **characterized in that** the communication apparatuses are adapted to communicate under the control of the TCP/IP protocol particularly suitable for a local area network.

9. System for data communication as claimed in claim 1 or 8, **characterized in that** at least one of the apparatuses is formed by a network of communication equipment.

10. System for data communication as claimed in claim 1, **characterized in that** at least a part of the network is formed by a digital radio network.

11. System for data communication as claimed in claim 1 or 10, **characterized in that** the network is adapted to communicate under the control of the MPAK protocol particularly suitable for a digital radio network.

12. System for data communication as claimed in claim 1, 10 or 11, **characterized in that** the network is adapted to effect error-free transfer of data by means of a check sum in only the MPAK protocol.

13. Gate device for use in a system as claimed in one or more than one of the foregoing claims, which gate device comprises: a processing unit, a memory means, input and output means for connection to one or more than one communication apparatus or to one or more than one other network, **characterized in that** the gate device is adapted to code or decode the apparatus protocol information placed in a packet together with the data for transfer and to add network protocol information to the packet or remove it therefrom.

14. Packet of data and protocol information for digital communication in a system as claimed in one or more than one of the foregoing claims, **characterized in**

that during transfer between a communication apparatus and a gate device the packet comprises complete information for the apparatus protocol and the complete data for transfer, and that during transfer through the network the packet comprises complete information for the network protocol, coded information for the apparatus protocol and coded data, wherein the first packet for transfer through the network further contains the coding information.

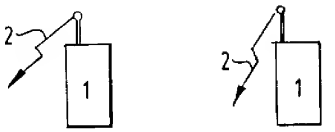


FIG.1

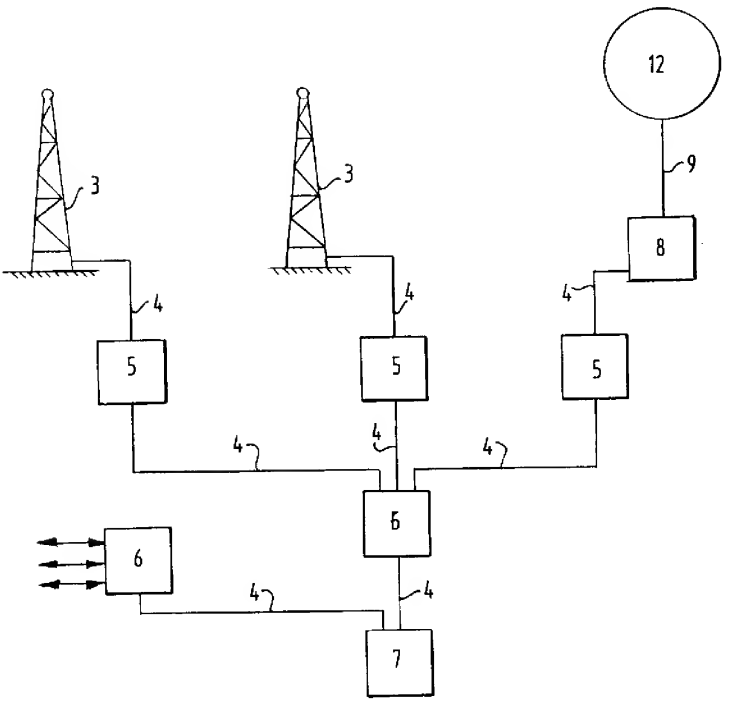
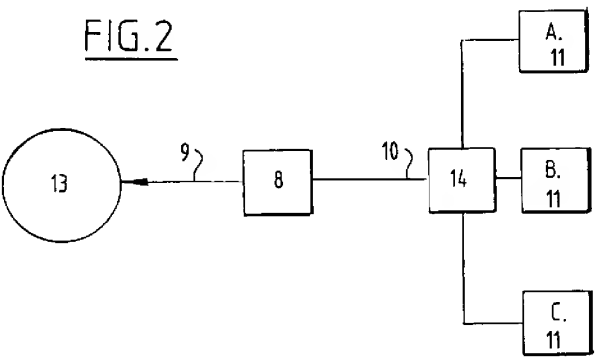


FIG.2



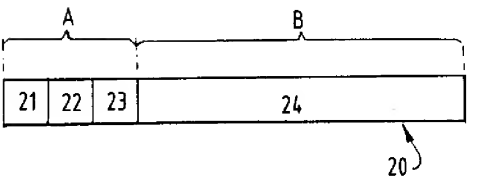


FIG.3

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : **H04L 12/28** — **A3**

(11) International Publication Number: **WO 96/11538**

(43) International Publication Date: 18 April 1996 (18.04.96)

(21) International Application Number: PCT/NL95/00334

(22) International Filing Date: 3 October 1995 (03.10.95)

(30) Priority Data:
9401626 4 October 1994 (04.10.94) NL

(71) Applicant *(for all designated States except US)*: MULTI-HOUSE AUTOMATISERING B.V. [NL/NL]; Doesburg-weg 7, NL-2803 PL Gouda (NL).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: HARDENDOOD, Theo [NL/NL]; Vredebest 15, NL-2801 AS Gouda (NL).

(74) Agent: 't JONG, Bastiaan, Jacobus; Arnold & Siedsma, Sweelinckplein 1, NL-2517 GK The Hague (NL).

(81) Designated States: AM, AU, BB, BG, BR, BY, CA, CN, CZ, EE, FI, GE, HU, IS, JP, KG, KP, KR, KZ, LK, LR, LT, LV, MD, MG, MN, MX, NO, NZ, PL, RO, RU, SG, SI, SK, TJ, TM, TT, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ, UG).

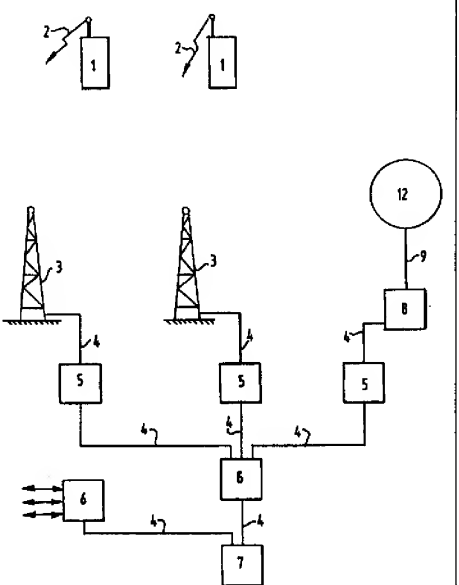
Published
With international search report.

(88) Date of publication of the international search report:
1 August 1996 (01.08.96)

(54) Title: SYSTEM FOR DIGITAL COMMUNICATION

(57) Abstract

The invention relates to a system for digital communication of data divided into packets between at least two communication apparatuses via a network, said network comprising at least two media, wherein communication in the network is controlled by a network protocol and communication between the apparatuses is controlled by an apparatus protocol. Unabbreviated and complete transfer through the network of data and apparatus protocol information supplemented with network protocol information results in unnecessarily bulky packets, since at least some of the functions of the apparatus protocol are likewise executed by the network protocol, wherein the cost of the transfer through the network is directly proportional to the number of packets for transfer and the size of these packets. The invention has for its object to obviate the above stated drawbacks and provides to this end a system which is distinguished in that between the network and at least one of the apparatuses is placed a gate device (8) which is adapted to code or decode the apparatus protocol information contained in a packet together with the data for transfer and to add network protocol information to the packet or remove it therefrom, and the system is further distinguished in that the gate device is adapted to transmit to an apparatus a confirmation to acknowledge receipt of a packet transmitted by this apparatus and to transfer the packet to the network for further transmission to the destination apparatus.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**GB**	United Kingdom	**MR**	Mauritania
AU	Australia	**GE**	Georgia	**MW**	Malawi
BB	Barbados	**GN**	Guinea	**NE**	Niger
BE	Belgium	**GR**	Greece	**NL**	Netherlands
BF	Burkina Faso	**HU**	Hungary	**NO**	Norway
BG	Bulgaria	**IE**	Ireland	**NZ**	New Zealand
BJ	Benin	**IT**	Italy	**PL**	Poland
BR	Brazil	**JP**	Japan	**PT**	Portugal
BY	Belarus	**KE**	Kenya	**RO**	Romania
CA	Canada	**KG**	Kyrgyzstan	**RU**	Russian Federation
CF	Central African Republic	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CG	Congo			**SE**	Sweden
CH	Switzerland	**KR**	Republic of Korea	**SI**	Slovenia
CI	Côte d'Ivoire	**KZ**	Kazakhstan	**SK**	Slovakia
CM	Cameroon	**LI**	Liechtenstein	**SN**	Senegal
CN	China	**LK**	Sri Lanka	**TD**	Chad
CS	Czechoslovakia	**LU**	Luxembourg	**TG**	Togo
CZ	Czech Republic	**LV**	Latvia	**TJ**	Tajikistan
DE	Germany	**MC**	Monaco	**TT**	Trinidad and Tobago
DK	Denmark	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**US**	United States of America
FI	Finland	**ML**	Mali	**UZ**	Uzbekistan
FR	France	**MN**	Mongolia	**VN**	Viet Nam
GA	Gabon				

INTERNATIONAL SEARCH REPORT

Interna al Application No
PCT/NL 95/00334

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO,A,94 08415 (CORAL NETWORK CORPORATION) 14 April 1994 see page 3, line 1 - line 26 see page 8, line 1 - page 11, line 7 see page 13, line 12 - page 14, line 5 see figures 1,3,4	1,6,8,9, 13,14
Y		5,10
Y		11,12
Y		8

Y	EP,A,0 597 640 (NCR INTERNATIONAL INC.) 18 May 1994 see column 2, line 52 - column 3, line 34 see column 6, line 2 - line 43 see column 7, line 2 - line 18 see column 8, line 16 - line 28 see figure 1 see abstract	5,10

	-/--	

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
7 May 1996	24.05.96
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Authorized officer Canosa Areste, C

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEE COLLOQUIUM ON CORDLESS COMPUTING - SYSTEMS AND USER EXPERIENCE, 12 January 1993, LONDON, GB, pages 1-5, XP002002261 J.B.HOLLIS: "AIR INTERFACE PROTOCOLS FOR A NATIONAL MOBILE DATA NETWORK" see the whole document	11,12
A		1-10,13, 14

Y	ELEKTROTECHNIK UND INFORMATIONSTECHNIK, vol. 110, no. 10, 1993, WIEN AT, pages 575-587, XP000403443 H.PICHLER: "KOMMUNIKATION ZWISCHEN LOKALEN NETWERKEN DURCH WEITVERKEHRSNETZE MIT MULTIPROTOKOLLROUTERN" see paragraph 8	8
A		1-7,9-14

INTERNATIONAL SEARCH REPORT

Intern[illegible]al Application No
PCT/NL 95/00334

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
WO-A-9408415	14-04-94	US-A-	5490252	06-02-96
EP-A-597640	18-05-94	JP-A-	7312597	28-11-95
		US-A-	5339316	16-08-94

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 29/06, 12/26 — A1

(11) International Publication Number: **WO 97/17790**

(43) International Publication Date: 15 May 1997 (15.05.97)

(21) International Application Number: PCT/FI96/00598

(22) International Filing Date: 6 November 1996 (06.11.96)

(30) Priority Data:
955355 7 November 1995 (07.11.95) FI

(71) Applicant *(for all designated States except US)*: NOKIA TELECOMMUNICATIONS OY [FI/FI]; Upseerinkatu 1, FIN-02600 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: RÄSÄNEN, Juha [FI/FI]; Pensaskertuntie 8 A, FIN-02660 Espoo (FI).

(74) Agent: OY KOLSTER AB; Iso Roobertinkatu 23, P.O. Box 148, FIN-00121 Helsinki (FI).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

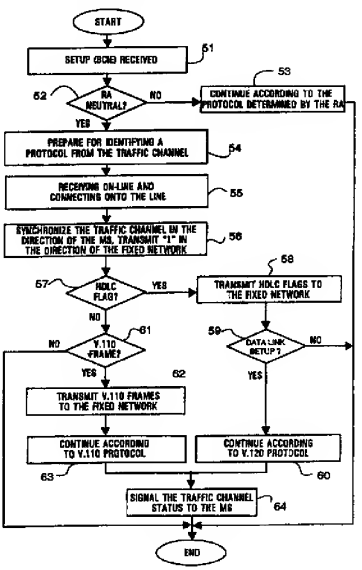
With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: ADAPTING THE FIXED NETWORK PROTOCOLS TO A MOBILE COMMUNICATIONS NETWORK

(57) Abstract

The invention relates to an interworking function apparatus (IWF), a method and an arrangement for establishing a mobile-terminating call in a mobile communications network when the call is received from a calling party via a fixed network without any signalling support which provides information on the protocol employed by the calling party. In the invention, a service is assigned only one directory number, which is common to all the protocols employed by the service. The protocol identifier in a service definition linked with this directory number has a neutral (undefined) value or may be interpreted as neutral. The IWF, upon receiving the neutral RA parameter (Step 2), is switched onto the line and monitors a traffic channel received from the fixed network in order to identify the protocol employed by the calling terminal equipment (Steps 54-57). After identifying the protocol, the IWF is configured according to the identified protocol (Steps 58-60 or 61-63), and data transfer may begin (Step 64).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

Adapting the fixed network protocols to a mobile communications network

Field of the Invention

The invention relates to a method and an arrangement for establishing a mobile-terminating call in a mobile communications network when the call is received from a calling party via a fixed network without any signalling support for carrying information on the protocol employed by the calling party.

Background of the Invention

Present-day mobile communications systems provide the subscribers, in addition to standard speech transmission, with a variety of data transfer features. The data services usually employ a certain specified communication protocol within the mobile network. In the pan-European digital mobile communication system GSM (Global System for Mobile Communications), for instance, a CCITT V.110 -based, UDI coded rate adaptation protocol is employed, and, in addition, a radio link protocol (RLP) is employed in non-transparent services. A digital connection from a mobile network to a fixed network, such as an ISDN (Integrated Services Digital Network) or a public switched telephone network PSTN, may employ different kinds of protocols. Examples of such protocols are the rate adaptation protocols CCITT V.110 and V.120 of the ISDN network.

An important feature related to data transfer services are adaptation functions for adapting the internal data connection within the mobile network to the protocols employed by the terminal equipments and other telecommunications networks. Typically, the adaptation functions are a Terminal Adaptation Function TAF at the interface between a mobile station and a

data terminal connected thereto, and an Interworking Function IWF at the interface between the mobile network and another telecommunications network.

Mobile networks are expected to provide a wide range of data services of various kinds which support the commonest data transfer protocols of fixed telecommunications networks. Consequently, a separate IWF is also required for each data transfer protocol. The mobile network must know which data transfer protocol the terminal equipments wish to employ in each call in order that it would be able to select the correct IWF.

In a mobile-originating call (MOC) the mobile station signals the information on the protocol it wishes to be employed towards the fixed network and the called party. In GSM mobile communications system, for instance, the information on the desired protocol is in a Bearer Capability Information Element (BCIE) in a setup message. On the basis of this information, the IWF is configured to provide a suitable interworking function between the mobile network and the telecommunications network. In case signalling that supports transmitting the protocol information is employed on the entire connection between the mobile network and the called party, the information is also transmitted to the called party. The required signalling support is provided e.g. in ISDN networks (Integrated Services Digital Network). If such signalling support is not provided, it is the responsibility of the calling subscriber to select the correct protocol, that is, the calling subscriber must know the protocol of the called subscriber and select the protocol of the IWF accordingly. Signalling support is not available e.g. in the conventional public switched telephone network PSTN.

A mobile-terminating call (MTC) is more problematic. In case the required signalling support is available on the entire connection between the calling party and the mobile network, the protocol parameters of the calling subscriber are transmitted to the mobile network, which may configure the IWF according to them. In practice, however, signalling support is not always available over the entire connection. This is the case, for instance, when a call originates from the PSTN or has been routed via the PSTN. When the signalling support is not available, the mobile network should be able to obtain the information on the protocol required by the call in some other way.

A prior art approach to the problem is a Multi Numbering Scheme, in which a mobile subscriber has as many directory numbers (MSISDN) as he has different services to which he wishes to receive incoming calls. In accordance with the multinumbering scheme, the calling subscriber dials the directory number of the mobile subscriber according to the desired service. In the GSM system, the services of the subscribers are determined in a subscriber's home location register (HLR), in which other subscriber information is also stored permanently. The HLR is also used for storing information on the mapping between the directory numbers and the services of the subscribers. In the HLR, a specific BCIE element indicating the type of a call and the network resources and the protocol required for the call is also linked with the Mobile Subscriber ISDN Number (MSISDN). The IWF may be configured according to this information. According to the present recommendations, a subscriber has a separate MSISDN number for the V.110 protocol and a separate MSISDN number for the V.120 protocol.

For the network operator and the mobile

subscribers, such a vast number of services causes confusion and trouble. In order for the mobile subscriber to be able to carry out and receive calls requiring different protocols, he must subscribe to several different bearer services from the network operator. From the point of view of the network operator, it is in turn problematic that each user should require a plurality of directory numbers, which wastes the number space of the network. Furthermore, determining the services in the network databases consumes database capacity. The multinumbering scheme is thus a working, yet a poor solution.

Summary of the Invention

It is an object of the invention to provide a method and arrangement that allow protocol adaptation between the mobile communications system and the fixed network more efficiently as compared with the present multinumbering scheme in a case where no signalling support is provided, thus saving the number space and database capacity.

This is achieved with a method for establishing a mobile-terminating data call when the call is received from the calling party via a fixed network without signalling support carrying the information on the protocol employed by the calling party. The method is characterized by

receiving a call to a directory number of a subscriber, said directory number being assigned to a data service employing two or more alternative protocols towards the fixed network,

retrieving from the subscriber data a service definition linked with said directory number, the protocol parameter of said definition having a neutral value or a value that is interpreted as neutral,

assigning an interworking function resource in

accordance with said service definition, omitting the definition of the protocol due to said neutral value or the value that is interpreted as neutral,

monitoring by means of the assigned interworking function resource the traffic channel received from the fixed network,

identifying the protocol employed by the calling party on the basis of signalling characteristic thereof,

configuring said assigned interworking function resource to employ said identified protocol towards said calling party.

The invention also relates to providing an arrangement for establishing a mobile-terminating data call in a mobile communications network when the call is received from the calling party via a fixed network without signalling support carrying the information on the protocol employed by the calling party. The arrangement is characterized by

the subscriber database of the mobile communications network having one directory number defined for a subscriber's data service that employs two or more alternative protocols towards the fixed network, the protocol parameter of a service definition linked with said directory number having a neutral value or a value that is interpreted as neutral,

the mobile network being arranged, in a mobile-terminating call made to said directory number, to assign an interworking function apparatus according to the service definition, but to omit the configuration of the protocol employed towards the fixed network due to the neutral value of said protocol parameter or the value that is interpreted as neutral,

said assigned interworking function apparatus (IWF) being arranged to monitor a traffic channel

received from the fixed network, to identify the protocol employed by the calling party (TE) on the basis of signalling characteristic thereof, and to configure itself to employ said identified protocol towards said calling party.

It is yet another aspect of the invention to provide an interworking function apparatus for achieving a protocol adaptation between a mobile communications network and a fixed network when a call is received from the calling party via the fixed network without any signalling support carrying the information on the protocol employed by the calling party. The apparatus is characterized by

the interworking function apparatus being arranged, in a mobile-terminating call, to assign interworking function resources according to the service definition obtained from the subscriber database, but to omit the configuration of the protocol employed towards the fixed network if the protocol parameter of said service definition has a neutral value or a value that is interpreted as neutral,

the interworking function apparatus being arranged to monitor a traffic channel received from the fixed network, to identify the protocol employed by the calling party on the basis of signalling characteristic thereof, and to configure said assigned interworking function resources to employ said identified protocol towards said calling party.

In the invention, a service is assigned only one directory number which is common to all the protocols employed by the service. In the service definition linked with this directory number, the protocol identifiers are neutral (undefined) in value or interpreted as neutral. When the interworking function (IWF) of the mobile network receives, in case

of a mobile terminating data call, a protocol identifier which is neutral or interpreted as neutral, it does not attempt, after being switched to the line, to synchronize itself towards the fixed network according to any protocol, but it monitors the traffic channel received from the fixed network in order to identify the protocol employed by the calling terminal equipment. The IWF, however, synchronizes the internal data connection within the mobile network in the specified way in the direction of the mobile station. After identifying the protocol of the calling terminal equipment, the IWF starts to operate in the manner required by the identified protocol. After setting up a data link, the IWF signals the status of the traffic channel to the mobile station in the usual way, and data transmission may begin.

Identifying the protocol is based on detecting synchronization or signalling characteristic thereof. The CCITT V.110 protocol may be identified by means of a V.110 synchronization frame. After identifying the V.110 synchronization frame, the IWF itself starts transmitting V.110 synchronization frames to the fixed network. The CCITT V.120 protocol may also be identified by means of a V.120 frame flag, in addition to which the identification may be confirmed by means of a link setup message. After identifying a V.120 frame flag, the IWF itself starts transmitting frame flags to the fixed network, and after identifying the link setup message, it acknowledges the message etc.

Brief Description of the Drawings

In the following, the invention will be explained by means of preferred embodiments with reference to the attached drawings, in which

Figure 1 illustrates a mobile communications system in which the present invention may be applied,

Figure 2 is a schematic block diagram of a mobile services switching centre provided with an interworking function apparatus IWF,

Figure 3A is a signalling diagram illustrating the first part of call establishment in a mobile-terminating UDI call which is made to an MSISDN number of an asynchronic service of a mobile station from a terminal equipment of a fixed network,

Figure 3B is a signalling diagram illustrating the latter part of call establishment shown in Figure 3A, the protocol of the terminal equipment being V.120,

Figure 3C is a signalling diagram illustrating the latter part of call establishment shown in Figure 3A, the protocol of the terminal equipment being V.110, and

Figure 4 is a flow chart illustrating monitoring of the traffic channel and identifying the protocol carried out by the IWF.

The present invention may be used in all digital mobile communication systems in which data services employ two or more kinds of different protocols towards the fixed network, such as ISDN or PSTN.

The present invention is particularly well suited for data transmission applications in the Pan-European digital mobile communication system GSM (Global System for Mobile Communications) and other GSM-based systems, such as DCS1800 (Digital Communication System), and the digital cellular system PCS (Personal Communication System) in the USA. The invention will be disclosed below by way of example of the GSM mobile communications system. The structure and operation of the GSM system are well known to a person skilled in the art, and they are specified in the ETSI (European Telecommunications Standards Institute) GSM

specifications. Reference is also made to "GSM System for Mobile Communication" by M. Mouly and M. Pautet, Palaiseau, France, 1992; ISBN 2-9507190-0-7.

The basic structure of the GSM system is illustrated in Figure 1. The GSM structure consists of two parts: a base station system BSS and a network subsystem (NSS). The BSS and the mobile stations MS communicate over radio connections. In the BSS, each cell is served by a base station BTS. A group of base stations is connected to a base station controller BSC, whose purpose is to control the radio frequencies and channels used by the BTS. The BSCs are connected to a mobile services switching center MSC. Specific MSCs are connected to other telecommunication networks, such as the PSTN, and comprise gateway functions for calls to and from these networks. These MSCs are known as gateway MSCs (GMSC).

There are two main classes of databases, associated with call routing. A home location register HLR permanently or semi-permanently stores the subscriber data of all the subscribers of the network, including information on the services the subscriber may have access to, and on the subscriber's current location. The second register type is a visitor location register VLR. The VLR is usually associated with one MSC, but it may, however, serve several MSCs. It is common practice that the VLR is integrated into the MSC. The integrated network element is known as a visitor MSC (VMSC). Whenever the mobile station MS is active (registered and capable of making or receiving calls), the majority of the mobile subscriber information concerning the MS and stored in the HLR is copied to the VLR of the particular MSC in whose service area the MS is located.

Still referring to Figure 1, a data link is

established in the GSM system between a mobile station MS network terminal TAF (Terminal Adaptation Function) 31 and a network adaptor IWF (Interworking Function) 41 in the mobile communication network. In the GSM network, the data link in data transfer is a V.110 rate adapted, V.24 interface compatible, UDI coded digital Full Duplex connection. In this connection, the V.110 connection is a digital transmission channel originally developed for ISDN (Integrated Services Digital Network). The transmission channel adapts to the V.24 interface and also provides a possibility for transfer of V.24 statuses (control signals). The CCITT recommendation for a V.110 rate-adapted connection is specified in the recommendation CCITT Blue Book: V.110. The CCITT recommendation for a V.24 interface is disclosed in the CCITT Blue Book: V.24. In non-transparent data services, a radio link protocol RLP is also employed. The terminal adaptor TAF adapts a data terminal equipment DTE connected to the MS for the V.110 connection, which is established over a physical connection using one or more traffic channels. The IWF couples the GSM V.110 connection to another V.110 or V.120 network such as an ISDN or another GSM network, or to another transit network, such as the public switched telephone network PSTN. The CCITT recommendation for a V.120 rate-adapted connection is specified in the recommendation CCITT White Book: V.120.

As it was explained above, modern mobile communication systems support different kinds of teleservices and bearer services. The bearer services of the GSM system are specified in the specification GSM 02.02 Version 4.2.0, and the teleservices in the specification GSM 0.0.3 Version 4.3.0.

The network adaptor IWF is often placed at the

MSC. Figure 2 illustrates a network adaptor apparatus placed at the MSC, carrying out the adapting to the PSTN and the data services of the ISDN network. For adapting to the PSTN, an ISDN 3.1 kHz audio service or another GSM network, the IWF comprises a group of baseband data modems 41A, which also include a rate adaptor. The modems 41A are autobauding modems capable of handshaking any data rate supported by the GSM system between 300-9600 bit/s, or for HSCSD data services even higher transfer rates, such as 14.4-28.8 kbit/s. Data modem 41A is used e.g. when a data connection is required via an analog PSTN to a data terminal TE of a fixed network or to an ISDN network with a 3.1 kHz audio service. In such a case, there is a similar data modem at the other end of the analog modem connection. There may be any required number of data modems, although Figure 2 only shows one modem 41A for the sake of clarity. The analog side of the modem 41A is connected via an exchange termination ET and the digital side is connected directly to a group switch GSW21 of the MSC. In addition, digital transfer links transmitted via the exchange terminations to the base station systems BSS are coupled to the group switch 21. Furthermore, via the exchange terminations ET, the transmissions channels of other telecommunication networks, such as ISDN or PSTN, are coupled to the group switch 21. The interworking function apparatus IWF of Figure 2 further comprises, for adapting to the Unrestricted Digital Information service UDI of the ISDN network, a data interface unit DIU 41B which comprises a rate adaptor. The DIU is used in GSM data calls to adapt the user data, rate adapted according to the V.110 or V.120 protocol, from the ISDN, as well as the status and control information according to the V.110 or V.120 protocol to the GSM traffic channel, and

in the opposite direction, the user data from the GSM traffic channel as well as the status and control information to the V.110 and V.120 frame structure of the ISDN. The ISDN side of the DIU 41B is connected via the exchange terminal ET, and the GSM side directly to the group switch GSW21. Although only one DIU 41B is shown in Figure 2, there may be any number of them depending on the capacity requirements. The group switch GSW21 and the interworking function apparatus IWF, as well as data call establishing, maintaining and releasing are all controlled by a call control 42. The operation of the IWF is controlled by an IWF control unit 41C which, under control of the call control 42, connects a network adaptor, i.e. the modem 41A or DIU 41B, required by the bearer service used by a particular data call to the data connection. In Figure 2, a solid line illustrates connecting the modem 41A, and a broken line illustrates connecting the DIU 41B. As an example of a mobile services switching center comprising such a network adaptor apparatus, the Nokia Telecommunication Ltd DX200 MSC can be mentioned.

As stated above, a mobile subscriber may traditionally have been entitled to different teleservices and bearer services each having a separate directory number MSISDN. In other words, each subscriber has had several MSISDN numbers. In addition, it has been necessary to determine every teleservice and bearer service of every subscriber in the subscriber's HLR in connection with other subscriber data, and to transfer them to the VLR. In the subscriber data, every MSISDN number is associated with a GSM system BCIE value, either directly or by means of an index pointing to a BCIE values chart. The BCIE is an information element used by the GSM system to transfer information on all the network requirements

related to the call, such as transfer rates, number of data and end bits, etc. The BCIE is described in, for example, the GSM specification 04.08, version 4.5.0, pp. 423-431.

In the invention, a service is assigned only one directory number MSISDN, which is common to all the protocols employed by the service. The service definition linked with this MSISDN number is stored in the HLR along with the other subscriber data. In this service definition, a GSM BCIE is linked with the MSISDN number. In the GSM BCIE the parameter RA (Rate Adaptation) that determines the rate adaptation protocol in the GSM BCIE has a neutral (undefined) value, or a value that may be interpreted as neutral. Presently, the parameter RA may determine the following cases: no rate adaptation, V.110/X.30 rate adaptation, X.31 flag stuffing, V.120. Furthermore, there are free values one of which may be selected as the neutral value in accordance with the invention. A neutral value of the parameter RA herein generally refers to a value which does not define any protocol for the IWF, but, as a result of which the MSC/IWF attempts to identify the protocol of a terminal equipment of a fixed network from the traffic channel. The MSC/IWF may also be arranged to interpret specific values of the RA parameter, such as V.110 and V.120, as neutral.

When the IWF obtains in connection of a terminating data call a neutral value of the RA parameter or a value that may be interpreted as neutral, it does not attempt to operate according to any protocol after switching to the line, until it has identified, by monitoring the traffic channel from the fixed network, the protocol employed by the calling terminal equipment.

In the following, establishing a MT call

according to the invention will be explained with reference to Figures 3A-C and 4. In the example, the service is an asynchronous UDI service, the different protocols employed by the service being V.110 and V.120. It must be noted, however, that the invention is not limited to these protocols, but it generally applies to any protocol.

The signalling diagrams of Figures 3A-C are related to an exemplary case in which a mobile-terminating (MT) UDI call is made from a fixed terminal equipment TE to the MSISDN number of a mobile subscriber, said number being assigned to an asynchronous data service of the subscriber. In such a case, the call is received in the mobile network from an ISDN network, but signalling support is not available on the entire connection between the mobile network and the terminal equipment TE for transmitting the protocol information. The first part of call establishment is illustrated in Figure 3A, and it is similar for both protocols. Figures 3B and 3C illustrate the latter part of call establishment in a case where the terminal equipment TE is employing V.120 protocol and V.110 protocol, respectively.

In Figure 3A, an IAM message (Initial Address Message) is transmitted from an ISDN network to a gateway MSC (GMSC) of the mobile network in a call made to a directory number MSISDN of a mobile subscriber's asynchronous service. The GMSC carries out a routing information request Send Routing Info to the subscriber's HLR, which is determined on the basis of the called MSISDN. Along with the routing information request, the subscriber's MSISDN number is also transmitted. The HLR retrieves from the subscriber data the GSM BCIE linked with the called directory number MSISDN. In this GSM BCIE the parameter ITC (Information

Transfer Capability) has the value UDI and the parameter RA has a neutral value, or a value that may be interpreted as neutral, e.g. V.110. The HLR then transmits the VLR a roaming number request Provide MSRN containing said GSM BCIE. The VLR stores the GSMBCIE and allocates the call a roaming number MSRN. The MSRN is transmitted to the HLR, which forwards it to the GMSC. The GMSC routes the call on the basis of the roaming number MSRN to the MSC in the area of which the mobile subscriber MS is located. The MSC then requests information from the VLR for establishing a mobile-terminating call on the basis of the roaming number MSRN. On the basis of the MSRN, the VLR retrieves the BCIE which was previously received from the HLR, and transmits it to the MSC. Following this, the MSC transmits the MS a call set-up message 'setup', which also contains the GSM BCIE. The MS replies with a 'call confirm' message. Subsequently, the MSC request the BSS with an 'Assignment Request' message to assign the required radio channels, and the BSS acknowledges with an 'Assignment Complete' message. Thereafter, the MSC allocates the required IWF resources by transmitting the IWF an 'IWF Setup' message, which also contains the GSM BCIE obtained from the VLR. At this stage, the operation of the IWF according to the invention begins, illustrated by means of the block diagram in Figure 4.

In step 51 in Figure 4, an IWF control unit 41C (Figure 2) receives from call control 42 of the MSC a SETUP message that contains the BCIE. IWF control unit 41C analyses the BCIE and, upon detecting that the ITC is an UDI, assigns the call a DIU 41B. In addition, the IWF checks the value of the RA parameter (step 52). Provided that the value of the RA parameter is neutral or can be interpreted as neutral, e.g. V.110 or V.120, the IWF control unit does not configure the DIU 41B for

any protocol, but prepares for monitoring a traffic channel received from the fixed network (step 54). Provided that, in step 52, it is detected that the value of the parameter RA is other than neutral or it cannot be interpreted as neutral, the IWF control unit 41C configures the DIU 41B in accordance with the protocol (53) determined by the parameter RA. Again with reference to Figure 3, the IWF acknowledges the allocation of the resources with a message 'acknowledgement'. The MS report with a message 'alerting' that alerting the calling subscriber has been started. The MSC, in turn, transmits the calling terminal equipment TE of the fixed network a message 'address complete' indicating that the connection has been established. The MSC then transmits a message 'connect' indicating that the called subscriber accepts the call, as a result of which the MSC transmits a message 'answer signal' to the calling terminal equipment TE. The MSC then controls the IWF with a message 'device on line'. It is thus returned to the operation of the IWF in accordance with the invention, described in Figure 4.

Again with reference to Figure 4, the IWF control unit 41C (Figure 2) receives from the call control 42 of the MSC a message 'device on line', as a result of which it connects the DIU 41B between the traffic channel received from the GSW21 BSS and the traffic channel received from the PSTN, as shown in Figure 2 with a broken line. Following this, the operation of the IWF continues in accordance with the flow chart in Figure 4.

With reference to Figure 4, after the IWF has been connected onto the line, synchronization of the GSM traffic channel is carried out between the TAF and the IWF in the usual way, and the IWF control unit 41C

starts to monitor the traffic channel received from the fixed network by means of the DIU 41B. The DIU 41B may thereby transmit a string of 1-bits to the traffic channel in the direction of the fixed network because this procedure is the same regardless of whether the calling terminal equipment TE employs a V.110 or V.120 protocol (step 56). Subsequently, the IWF control unit 41C checks whether the signalling received from the terminal equipment TE contains a frame flag typical of V.120 protocol, that is, a HDLC flag 01111110 (step 57). If it does, this is followed by signalling according to Figure 3B.

The IWF transmits HDLC flags to the terminal equipment TE of the fixed network (step 58, Figure 4). As transmitting HDLC flags may be a part of some other protocol than V.120, the IWF control unit 41C checks in the preferred embodiment of the invention whether a data link setup message characteristic of the V.120 protocol is received from the terminal equipment TE (step 59). If the data link setup message is received, the IWF control unit 41C configures the DIU 41B to employ the V.120 protocol, and the IWF begins to operate in the direction of the fixed network in the manner required by the V.120 protocol (step 60). This includes transmitting an acknowledgement to the data link setup message to the terminal equipment TE. Thereafter, the IWF signals a normal traffic channel status to the NS, and data transfer may begin (step 64).

If the data link setup message is not received in step 59, protocol identification is regarded as failed in this embodiment of the invention, and it is proceeded to the end.

Provided that the HDLC flag is not received in step 57 of Figure 4, the IWF control unit 41C checks

whether the signalling received from the fixed network contains a V.110 synchronization frame (step 61). If a V.110 synchronization frame is received, signalling proceeds in the manner described in Figure 3C. In other words, after identifying V.110 protocol by means of the V.110 synchronization frame, the IWF control unit 41C configures the DIU 41B in accordance with the identified V.110 protocol. Thereafter, the IWF transmits V.110 synchronization frames to the terminal equipment TE to the fixed network (step 62, Figure 4). The IWF then continues the operation in accordance with V.110 protocol in the direction of the terminal equipment TE (step 63) and signals the status of the traffic channel to the MS in the usual way by using V.24 statuses (step 64).

In case a V.110 frame is not received in step 61, protocol identification is interpreted as failed in this embodiment and it is proceeded to the end.

The figures and the explanation associated therewith are only intended to illustrate the resent invention. In its details, the invention may vary within the scope and the spirit of the attached claims.

Claims:

1. A method and arrangement for establishing a mobile-terminating call in a mobile communications network when the call is received from a calling party via a fixed network without any signalling support carrying information on the protocol employed by the calling party, c h a r a c t e r i z e d by

receiving a call to a directory number of a subscriber, said directory number being assigned to a data service employing two or more alternative protocols towards the fixed network,

retrieving from the subscriber data a service definition linked with said directory number, the protocol parameter of said definition having a neutral value or a value that is interpreted as neutral,

assigning an interworking function resource in accordance with said service definition, omitting the definition of the protocol due to said neutral value or the value that is interpreted as neutral,

monitoring by means of the assigned interworking function resource the traffic channel received from the fixed network,

identifying the protocol employed by the calling party on the basis of signalling characteristic thereof,

configuring said assigned interworking function resource to employ said identified protocol towards said calling party.

2. A method as claimed in claim 1, c h a r a c t e r i z e d by

identifying the protocol of the calling party as a CCITT V.110 rate adaptation protocol provided that a V.110 synchronization frame is received from the traffic channel,

configuring said assigned interworking function resource to employ V.110 protocol.

3. A method as claimed in claim 1, c h a r a c t e r i z e d by

identifying the protocol of the calling party as a CCITT V.120 rate adaptation protocol provided that a V.120 frame flag is received from the traffic channel,

configuring said assigned interworking function resource to employ V.120 protocol.

4. A method as claimed in claim 1, c h a r a c t e r i z e d by

receiving from the traffic channel a V.120 frame flag,

transmitting V.120 frame flags to another traffic channel,

identifying the protocol of the calling party as a CCITT V.120 rate adaptation protocol provided that a data link setup message according to V.120 protocol is received from the traffic channel,

configuring said interworking function resource to employ the V.120 protocol.

5. An arrangement for establishing a mobile-terminating data call in a mobile communications network when a call is received from a calling party (TE) via a fixed network (PSTN, ISDN) without signalling support that carries the information on the protocol employed by the calling party, c h a r a c t e r i z e d by

the subscriber database (HLR) of the mobile communications network having one directory number defined for a subscriber's data service that employs two or more alternative protocols towards the fixed network, the protocol parameter of a service definition linked with said directory number having a neutral

value or a value that is interpreted as neutral,

the mobile network being arranged, in a mobile-terminating (MS) call to said directory number, to assign an interworking function apparatus (IWF) according to the service definition, but to omit the configuration of the protocol employed in the direction of the fixed network (PSTN, ISDN) due to the neutral value of said protocol parameter or the value that is interpreted as neutral,

said assigned interworking function apparatus (IWF) being arranged to monitor a traffic channel received from the fixed network, to identify the protocol employed by the calling party (TE) on the basis of signalling characteristic thereof, and to configure itself to employ said identified protocol towards said calling party.

6. An arrangement as claimed in claim 5, c h a r a c t e r i z e d by the protocol employed by the calling party (TE) being a CCITT V.110 rate adaptation protocol, and said signalling characteristic of the protocol containing a V.110 signalling frame.

7. An arrangement as claimed in claim 5, c h a r a c t e r i z e d by the protocol employed by the calling party (TE) being a CCITT V.120 rate adaptation protocol, and said signalling characteristic of the protocol containing a V.120 frame flag or a V.120 data link setup message.

8. An interworking function apparatus of a mobile communication network for achieving a protocol adaptation when a call is received from the calling party via a fixed network without signalling support that carries the information on the protocol employed by the calling party, c h a r a c t e r i z e d by

the interworking function apparatus (IWF) being arranged, in a mobile-terminating (MS) call, to

assign interworking function resources according to the service definition obtained from the subscriber database, but to omit the configuration of the protocol employed towards the fixed network (PSTN, ISDN) if the protocol parameter of said service definition has a neutral value or a value that is interpreted as neutral,

the assigned interworking function apparatus (IWF) being arranged to monitor a traffic channel received from the fixed network, to identify the protocol employed by the calling party (TE) on the basis of signalling characteristic thereof, and to configure said assigned interworking function resources to employ said identified protocol towards said calling party (TE).

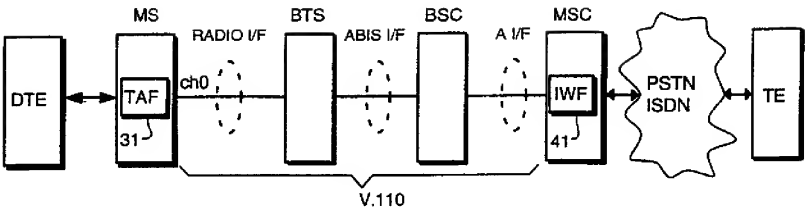

MS
RADIO I/F
BTS
ABIS I/F
BSC
A I/F
MSC
DTE
TAF
ch0
IWF
PSTN
ISDN
TE
31
41
V.110

Fig. 1

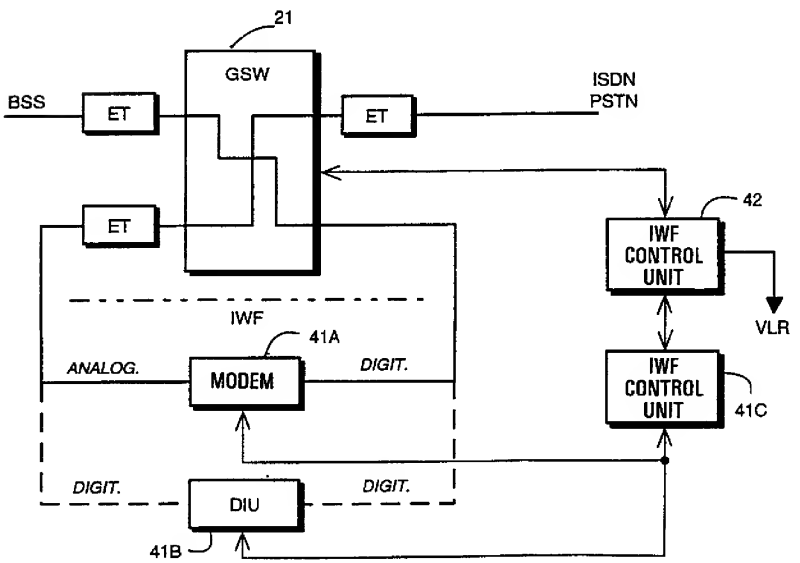

21
GSW
BSS
ET
ET
ISDN
PSTN
ET
42
IWF
CONTROL
UNIT
VLR
IWF
41A
ANALOG.
MODEM
DIGIT.
IWF
CONTROL
UNIT
41C
DIGIT.
DIU
DIGIT.
41B

Fig. 2

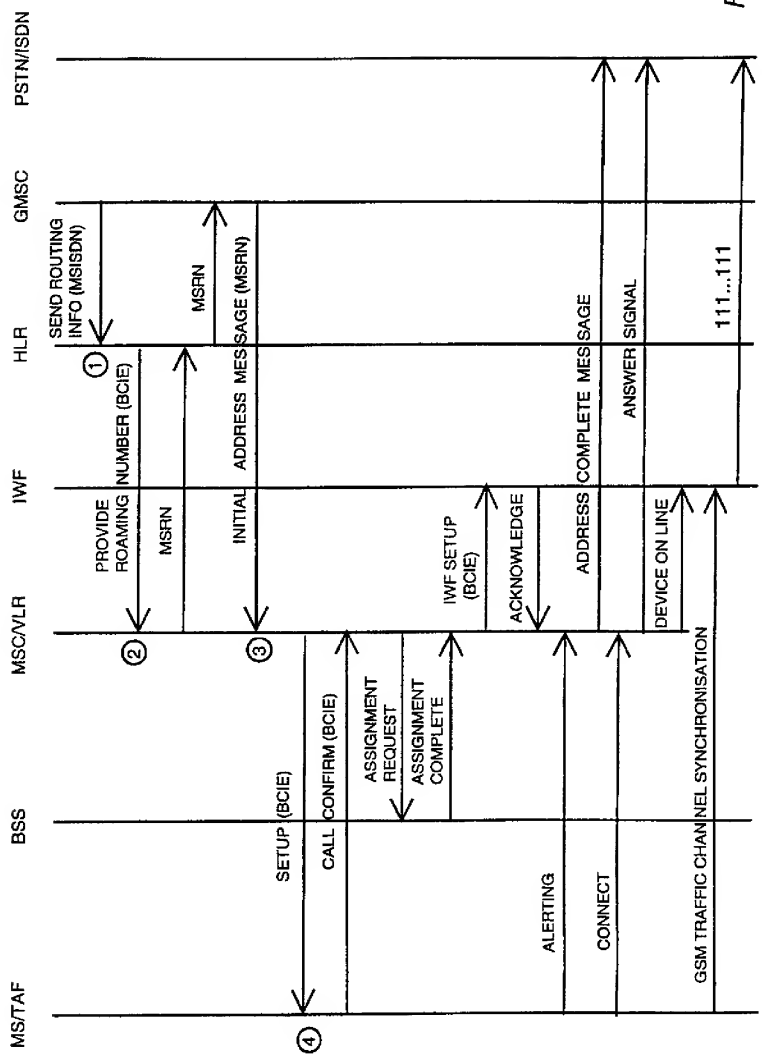

MS/TAF
BSS
MSC/VLR
IWF
HLR
GMSC
PSTN/ISDN
SEND ROUTING INFO (MSISDN)
1
PROVIDE ROAMING NUMBER (BCIE)
MSRN
2
MSRN
INITIAL ADDRESS MESSAGE (MSRN)
3
SETUP (BCIE)
CALL CONFIRM (BCIE)
ASSIGNMENT REQUEST
ASSIGNMENT COMPLETE
IWF SETUP (BCIE)
ACKNOWLEDGE
ADDRESS COMPLETE MESSAGE
ANSWER SIGNAL
DEVICE ON LINE
111...111
ALERTING
CONNECT
GSM TRAFFIC CHANNEL SYNCHRONISATION
4

Fig. 3A

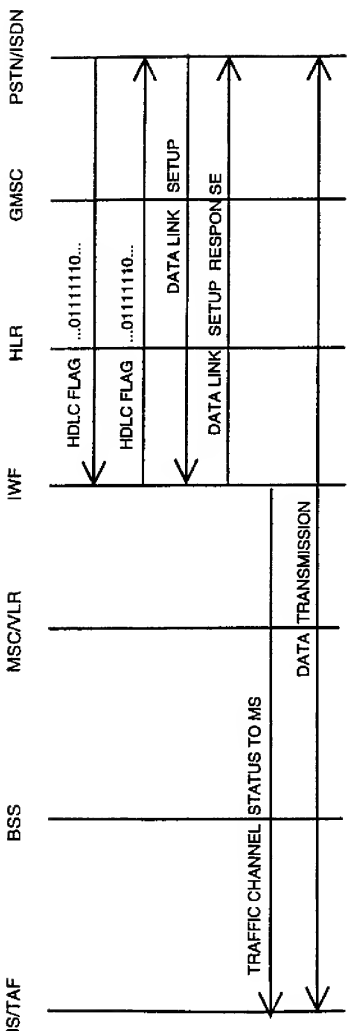

MS/TAF
BSS
MSC/VLR
IWF
HLR
GMSC
PSTN/ISDN
HDLC FLAG ...01111110...
HDLC FLAG ...01111110...
DATA LINK SETUP
DATA LINK SETUP RESPON SE
TRAFFIC CHANNEL STATUS TO MS
DATA TRANSMISSION

Fig. 3B

MS/TAF
BSS
MSC/VLR
IWF
HLR
GMSC
PSTN/ISDN
V.110 SYNCHRONISATION FRAMES
V.110 SYNCHRONISATION FRAMES
TRAFFIC CHANNEL STATUS TO MS
DATA TRANSMISSION

Fig. 3C

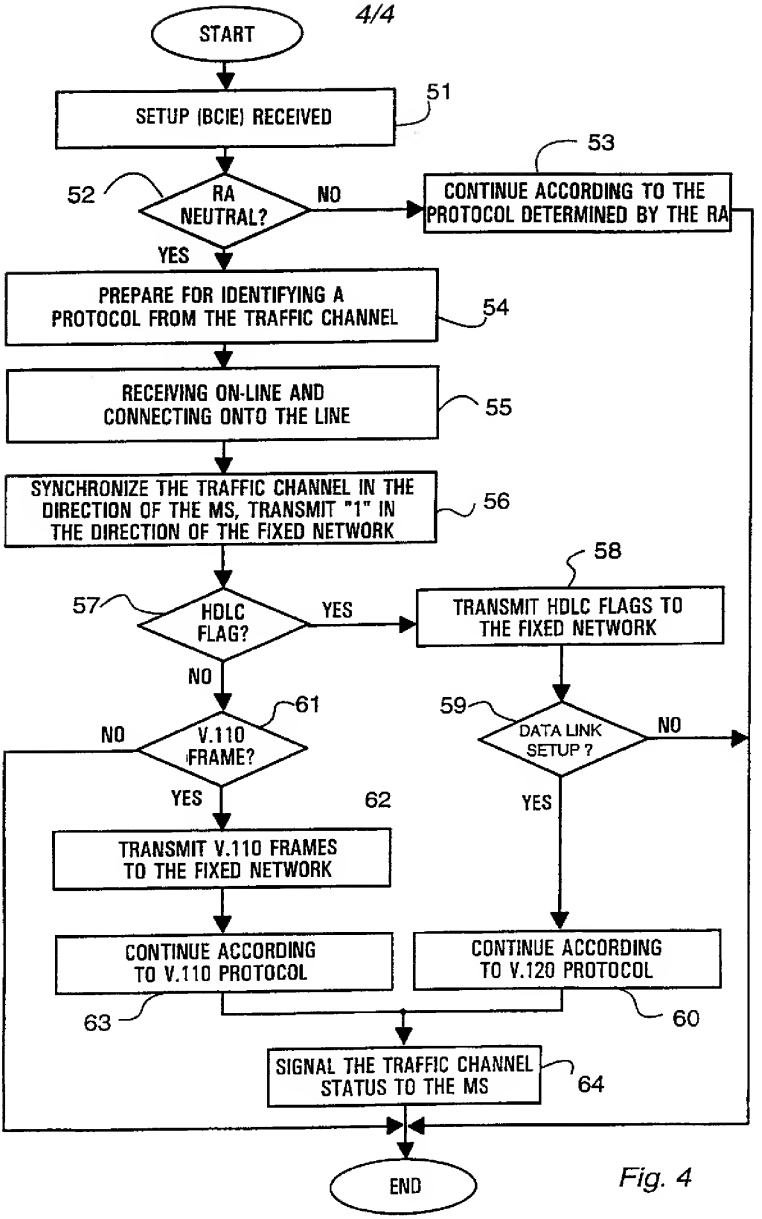

START
SETUP (BCIE) RECEIVED
51
RA NEUTRAL?
52
NO
CONTINUE ACCORDING TO THE PROTOCOL DETERMINED BY THE RA
53
YES
PREPARE FOR IDENTIFYING A PROTOCOL FROM THE TRAFFIC CHANNEL
54
RECEIVING ON-LINE AND CONNECTING ONTO THE LINE
55
SYNCHRONIZE THE TRAFFIC CHANNEL IN THE DIRECTION OF THE MS, TRANSMIT "1" IN THE DIRECTION OF THE FIXED NETWORK
56
HDLC FLAG?
57
YES
TRANSMIT HDLC FLAGS TO THE FIXED NETWORK
58
NO
V.110 FRAME?
61
NO
DATA LINK SETUP ?
59
NO
YES
YES
62
TRANSMIT V.110 FRAMES TO THE FIXED NETWORK
CONTINUE ACCORDING TO V.110 PROTOCOL
63
CONTINUE ACCORDING TO V.120 PROTOCOL
60
SIGNAL THE TRAFFIC CHANNEL STATUS TO THE MS
64
END

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00598

A. CLASSIFICATION OF SUBJECT MATTER

IPC6: H04L 29/06, H04L 12/26
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC6: H04L, H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

SE,DK,FI,NO classes as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0478175 A1 (HEWLETT-PACKARD COMPANY), 1 April 1992 (01.04.92), column 2, line 3 - column 3, line 33 --	1,5,8
A	US 5430709 A (JAMES R. GALLOWAY), 4 July 1995 (04.07.95), see the abstract --	1,5,8
A	US 4891783 A (AKITOSHI ARITAKA ET AL.), 2 January 1990 (02.01.90), see the whole document --	1,5,8
A	EP 0503487 A2 (STANDARD ELEKTRIK LORENZ AKTIENGESELLSCHAFT), 16 Sept 1992 (16.09.92), see the whole document --	1,5,8

[X] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" erlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 March 1997	13 -03- 1997
Name and mailing address of the ISA/ Swedish Patent Office Box 5055, S-102 42 STOCKHOLM Facsimile No. +46 8 666 02 86	Authorized officer Friedrich Kühn Telephone No. +46 8 782 25 00

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/FI 96/00598

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5282194 A (THOMAS J. HARLEY ET AL.), 25 January 1994 (25.01.94), column 1, line 63 - column 2, line 51; column 3, line 22 - column 5, line 27	1,5,8

INTERNATIONAL SEARCH REPORT
Information on patent family members

03/02/97

International application No.
PCT/FI 96/00598

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A1- 0478175	01/04/92	DE-D,T- 69114805	18/04/96
		EP-A- 0474932	18/03/92
		US-A- 5347524	13/09/94
US-A- 5430709	04/07/95	EP-A- 0598739	01/06/94
		JP-T- 6509927	02/11/94
		WO-A- 9326111	23/12/93
US-A- 4891783	02/01/90	JP-A- 62159947	15/07/87
EP-A2- 0503487	16/09/92	SE-T3- 0503487	
		AT-T- 127307	15/09/95
		AU-B- 641586	23/09/93
		AU-A- 1128992	17/09/92
		CA-A- 2062621	12/09/92
		DE-A- 4107742	17/09/92
		DE-D- 59203413	00/00/00
		ES-T- 2080976	16/02/96
		JP-A- 5083248	02/04/93
		US-A- 5311590	10/05/94
US-A- 5282194	25/01/94	NONE	

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
G06F 11/10, H04J 3/24, H04L 1/02, H04B 15/00, H04K 1/00

A1

(11) International Publication Number: **WO 99/30234**

(43) International Publication Date: 17 June 1999 (17.06.99)

(21) International Application Number: PCT/US98/24472

(22) International Filing Date: 16 November 1998 (16.11.98)

(30) Priority Data:
08/988,026 10 December 1997 (10.12.97) US

(71) Applicant: L-3 COMMUNICATIONS CORPORATION [US/US]; 600 Third Avenue, New York, NY 10016 (US).

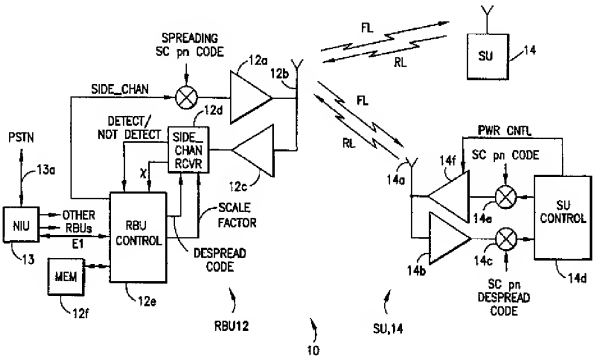
(72) Inventors: STEPHENSON, Philip, L.; 1121 Goodwin Circle, Salt Lake City, UT 84116 (US). GIALLORENZI, Thomas, R.; 7794 West Mt. Top Road, Herriman, UT 89065 (US). HARRIS, Johnny, M.; 80 W. 70 S., Centerville, UT 84014 (US). BUTTERFIELD, Lee, A.; 3093 W. Green Acre Drive, W. Jordan, UT 84088 (US). HURST, Michael, J.; 9862 S. Heavenly Circle, S. Jordan, UT 84095 (US). GRIFFIN, Dan; 1086 Oakridge Lane, Bountiful, UT 84010 (US). THOMPSON, Rolf; 1142 E. 470 N., Orem, UT 84097 (US).

(74) Agent: GREEN, Clarence, A.; Perman & Green, LLP, 425 Post Road, Fairfield, CT 06430 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: WAVEFORM AND FRAME STRUCTURE FOR A FIXED WIRELESS LOOP SYNCHRONOUS CDMA COMMUNICATIONS SYSTEM



(57) Abstract

Disclosed is a method for transmitting information in a CDMA communication system including (a) multiplexing (53) data and control information into a data stream; (b) encoding (54) the data stream to form a stream of encoded I/Q symbol pairs (62A, 62B); (c) inserting synchronization information into the stream of encoded I/Q symbols pairs; and (d) spreading the encoded I/Q symbol pairs and the inserted synchronization information using a same pseudonoise (pn) spreading code (14e) prior to transmission as a frame. The preferred frame structure includes an unencoded synchronization field followed by a plurality of multi-byte data field. Individual ones of the plurality of data fields (80A) are separated by a control message field (80B). Individual ones of the control message fields contain a single byte of a multi-byte control message frame (82).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

WAVEFORM AND FRAME STRUCTURE FOR A FIXED WIRELESS LOOP SYNCHRONOUS CDMA COMMUNICATIONS SYSTEM

FIELD OF THE INVENTION:

This invention relates generally to wireless local loop systems and, in particular, a fixed wireless loop system providing voice and data communications between a radio base unit and a plurality of subscriber stations.

BACKGROUND OF THE INVENTION:

Local loop by traditional definition is that portion of a network that connects a subscriber's home to a central office switch. This is, however, an expansive definition that does not hold true as the network extends into the local loop by means of Digital Loop Carrier and Digital Cross Connects. For the purposes of this invention, local loop is considered as the connection from the subscriber's premises to the connecting point in the network, whatever the nature of that connection may be.

Until recently the local loop was mostly based on copper plant supplemented by microwave radio links for remote areas or difficult terrain. Over the last decade fiber

optics have made significant inroads into the local loop (also referred to as "access" network) reaching closer to subscriber homes and buildings. Sonet based access networks bring fiber to the curb. These fiber based solutions can provide very high bandwidth services, reliably and cost-effectively, in urban/metropolitan areas with significant numbers of business customers. In fact, most access providers in the U.S. have used such fiber based plant to provide access services to U.S. business customers.

The copper and fiber based solutions, while economical in many situations, still suffer from a number of drawbacks.

For example, in an area without an existing network infrastructure, it is very time consuming and expensive to build a new network. The expense is primarily in the labor, rights acquisition (for right of way or easement), and in electronics (for fiber based access). Overall the process is very slow due to extensive effort involved in acquiring right of way and in performing the required construction, aerial and/or underground. Also, in locations with extensive but congested existing infrastructure, it is often very expensive to add capacity due to already full ducts and cables, and sometimes impossible to add capacity without resorting to upgrading the entire system. In addition, wireline solutions tend to have costs that are distance sensitive, hence they are inherently unsuitable for sparse/scattered demand. Wireline networks are also not amenable to redeployment, which results in stranded assets when demand (consumer) moves. Wireline networks also cannot be rapidly deployed in emergency situations.

The term "fixed wireless loop", or FWL, connotes a fixed wireless based local access. However, it is often mixed with limited mobility solutions under the broader term "Radio Access". Irrespective of the type of radio

technology, all fixed wireless or radio access systems use wireless means to provide network access to the subscriber. Broadly speaking, there are three main categories of fixed wireless solutions.

Fixed cellular systems are primarily based on existing analog cellular systems such as AMPS (in North America) or NMT (in Nordic countries).

Fixed cordless systems are primarily based on the European DECT standard using digital TDMA Time Division Duplex technology.

Bespoke systems are designed specifically for fixed wireless application. Conventional systems in this category are the analog microwave point to multi-point systems. More recently deployed systems operate at higher frequencies and employ digital technologies. These systems may be derived from similar cellular technologies, but are not based on any existing agreed upon standards.

Of the three main categories of fixed wireless systems there is no one solution that is clearly superior to others. If the primary need for a system operator is to provide voice oriented service wherein voice quality is not a limiting factor, then often a fixed cellular system is adequate, and even desirable because of its relatively low equipment cost. For very high density urban situations, a DECT solution may be desirable due to its high load carrying capacity and its pico-cellular architecture. Microwave solutions are best for sparse populations. Bespoke systems function well over a wide range of situations and have the best overall quality and desirable features, however they are likely to be more expensive, at least in the near future.

Most residential consumers in developing economies are mainly interested in adequate voice service. However, most business customers require data and fax service in addition to voice. With the growing popularity of home computers and Internet access, a need is arising to provide residential consumers with high speed data services at home. As such, the general trend is in the direction that all customers, both residential and business, will demand high quality voice and data services.

A problem that arises in conventional Code Division Multiple Access communications systems relates to system capacity constraints imposed by the finite number of available pseudonoise (pn) spreading codes. This problem is compounded when two pn codes are used in one channel for spreading (and despreading) the Inphase (I) and the Quadrature (Q) symbol pairs.

Another problem in conventional communication systems relates to the transmission of control messages. Typically, control messages are put on a queue for earliest transmission, and frame structures are typically designed to transmit all control messages for a particular frame in a single block either at the beginning or end of the frame. However, this approach adds a delay in order to transmit all control for a particular frame in a single block either at the beginning or end of the frame. For example, if a one byte message is at the top of the queue when a new frame ends, this message cannot be transmitted for an entire frame until the next block is ready to be sent. In this case, the delay would be an entire frame.

OBJECTS AND ADVANTAGES OF THE INVENTION:

It is a thus a first object and advantage of this invention to provide an improved fixed wireless loop system that

fulfills the foregoing and other needs and requirements.

It is a further object and advantage of this invention to provide an improved fixed wireless loop system that exhibits an improved use of pn codes, and that furthermore overcomes the control message related delay problem.

SUMMARY OF THE INVENTION

The foregoing and other problems are overcome and the objects and advantages are realized by methods and apparatus in accordance with embodiments of this invention.

Disclosed is a method for transmitting information in a CDMA communication system, the method including steps of (a) multiplexing data and control information into a data stream; (b) encoding the data stream to form a stream of encoded I/Q symbol pairs; (c) inserting synchronization information into the stream of encoded I/Q symbol pairs; and (d) spreading the encoded I/Q symbol pairs and the inserted synchronization information using a same pseudonoise (pn) spreading code prior to transmission as a frame.

The step of multiplexing forms a data stream having data fields comprised of a plurality of data bytes separated by control message fields each comprised of a single byte of a control message frame. The control message frame includes a control message header field, a plurality of control data fields, and a plurality of data integrity fields.

More particularly, the frame is comprised of an unencoded synchronization field followed by a plurality of data fields each comprised of a plurality of data bytes. Individual ones of the plurality of data fields are separated by a control message field. Individual ones of

the control message fields are comprised of a single byte of the multi-byte control message frame.

In the preferred embodiment of this invention the step of encoding includes steps of (a) rate 1/2 convolutionally encoding the data stream to form an I channel and a Q channel; and (b) rate 4/5 punctured trellis coding the I and Q channels.

BRIEF DESCRIPTION OF THE DRAWINGS

The above set forth and other features of the invention are made more apparent in the ensuing Detailed Description of the Invention when read in conjunction with the attached Drawings, wherein:

Fig. 1 is a simplified block diagram of a synchronous, DS-CDMA fixed wireless communications system in accordance with this invention, the system having a radio base unit (RBU) and a plurality of transceiver or subscriber units (SUs). The RBU transmits a side channel to the SUs, and also receives an essentially asynchronously transmitted side channel from the SUs.

Fig. 2 is an exemplary frequency allocation diagram of the system of Fig. 1.

Fig. 3 is a block diagram illustrating the RBU and SU of Fig. 1 in greater detail.

Fig. 4 illustrates a presently preferred frame structure having data fields interspersed with control message frame fields.

Figs. 5A and 5B illustrate portions of the RBU transmit and receiver circuitry, respectively, in greater detail.

DETAILED DESCRIPTION OF THE INVENTION

By way of introduction, and referring to Fig. 1, a Fixed Wireless System (FWS) 10 in accordance with a preferred embodiment of this invention is a bespoke system based on digital radio technology. Specifically, the FWS 10 employs direct sequence spread spectrum based CDMA techniques over an air link to provide local access to subscribers. It offers very high quality, highly reliable service at costs that are very competitive with wireline solutions. The FWS 10 exhibits high spectral efficiency and thus can provide good wireline quality service with limited available bandwidth. A large dynamic range allows the FWS 10 to be deployable in a pico, micro, or mini cellular architecture meeting specific needs of dense metropolitan, urban, and suburban communities in an economical way.

Some important attributes of the FWS 10 include: wireline voice quality delivered at 32 Kbps; high throughput for data and fax applications with 32/64 Kbps throughput; high service reliability with good tolerance for noise and ingress; secure airlink; and support of enhanced services such as priority/emergency calling, both inbound and outbound.

The FWS 10 has a three to five times capacity advantage over conventional asynchronous CDMA technologies, and a three to seven times capacity advantage over currently available Time Division Multiple Access (TDMA) technology, due to its ability to use a frequency reuse of one.

The FWS 10 is a synchronous CDMA (S-CDMA) communications system wherein forward link (FL) transmissions from a radio base unit (RBU) 12 for a plurality of transceiver units, referred to herein as user or subscriber units (SUs) 14, are symbol and chip aligned in time, and wherein the SUs 14

operate to receive the FL transmissions and to synchronize to one of the transmissions. Each SU 14 also transmits a signal on a reverse link (RL) to RBU 12 in order to synchronize the timing of its transmissions to the RBU 12, and to generally perform bidirectional communications. The FWS 10 is suitable for use in implementing a telecommunications system that conveys voice and/or data between the RBU 12 and the SUs 14.

The SU 14 forms a portion of a Customer Premises Equipment (CPE). The CPE also includes a Network Termination Unit (NTU) and an Uninterruptible Power Supply (UPS), which are not illustrated in Fig. 1.

The RBU 12 includes circuitry for generating a plurality of user signals (USER_1 to USER_n), which are not shown in Fig. 1, and a synchronous side channel (SIDE_CHAN) signal that is continuously transmitted. Each of these signals is assigned a respective pn spreading code and is modulated therewith before being applied to a transmitter 12a having an antenna 12b. When transmitted on the FL the transmissions are modulated in phase quadrature, and the SUs 14 are assumed to include suitable phase demodulators for deriving in-phase (I) and quadrature (Q) components therefrom. The RBU 12 is capable of transmitting a plurality of frequency channels. By example, each frequency channel includes up to 128 code channels, and has a center frequency in the range of 2 GHz to 3 GHz.

The RBU 12 also includes a receiver 12c having an output coupled to a side channel receiver 12d. The side channel receiver 12d receives as inputs the spread signal from the receiver 12c, a scale factor signal, and a side channel despread pn code. These latter two signals are sourced from a RBU processor or controller 12e. The scale factor signal can be fixed, or can be made adaptive as a function of the

number of SUs 14 that are transmitting on the reverse channel. The side channel receiver 12d outputs a detect/not detect signal to the RBU controller 12e for indicating a detection of a transmission from one of the SUs 14, and also outputs a power estimate value χ, as described below. A read/write memory (MEM) 12f is bidirectionally coupled to the RBU controller 12e for storing system parameters and other information, such as SU timing phase information and power estimate values.

A Network Interface Unit (NIU) 13 connects the RBU 12 to the public network, such as the public switched telephone network (PSTN) 13a, through analog or digital trunks that are suitable for use with the local public network. The RBU 12 connects to the NIU 13 using E1 trunks and to its master antenna 12b using a coaxial cable. The SU 14 communicates with the RBU 12 via the radio interface, as described above.

In addition, the FWS 10 has an Element Management System or EMS (not depicted) that provides Operations, Administration, Maintenance, and Provisioning (OAM&P) functions for the NIU 13 and RBU 12. The functioning of the EMS is not germane to an understanding of this invention, and will not be further described in any great detail.

The NIU 13 is the interface to the public network for the system 10. Its primary purpose is to provide the specific protocols and signaling that are required by the public network. These protocols can vary by country as well as by customer, and possibly even by the connecting point in the network.

In a preferred embodiment of this invention the NIU 13 can connect to a maximum of 15 RBUs 12 using one to four E1 connections per RBU 12, with four E1 connections being used

for a fully populated RBU 12. In addition, each NIU 13 is sized for up to, by example, 10,000 subscribers. Time Slot 16 on each E1 trunk is used for passing control information between the NIU 13 and the attached RBUs 12, as well as for passing information to and from the controlling EMS. The protocol is based on the HDLC format and optimized to enhance RBU-NIU communication.

Specific functions provided by the NIU 13 include: initialization of the RBU 12; provisioning of dial tone and DTMF to the SUs 14; set up and tear down of voice and data calls; maintenance of Call Detail Record (CDR) data; HDLC Protocol (data link protocol to RBU Link Control Processor); billing system interface; Common Channel Signaling (CCS) for ringing and onhook/offhook detection; glare detection in NIU, RBU, and SU; call priority management; channel reassignment for calls in progress; detection of hook flash to enable plain old telephone service (POTS) and enhanced POTS calling features; 32/64 Kbps rate change initialization; pay phone capability (12/16 KHz tone detection, line reversal); priority and emergency number calling; accommodation of country specific signaling interfaces such as E&M, R1, R2, R2 variants, and C7; and system modularity: analog/digital options for both line side and trunk side.

The normal mode of operation for the SU 14 is a compressed speech mode using ADPCM encoding according to the ITU-T G.721 standard. This toll quality, 32 Kbps service is the default used whenever a non-X.21 channel is established with the RBU 12 (X.21 channels are configured a priori when provisioned by the EMS/NIU). The 32 Kbps channels may be used for voice band data up to 9600 b/s if desired. When the channel rate bumps to 64 Kbps PCM encoded voice/data due to detection of a fax/modem start tone, fax and modem rates of at least 33.6 Kbps are possible.

The SU-RBU air link provides a separate 2.72 MHz (3.5 MHz including guardbands) channel in each direction separated by either 91MHz or 119 MHz of bandwidth. The nominal spectrum of operation is 2.1-2.3 GHz or 2.5-2.7 GHz. However, the system is designed such that the frequency can be varied from 1.8 to 5 GHz provided the spectral mask and separation between transmit and receive frequencies is maintained as per ITU 283.5 specification. As per the ITU 283.5 specification, there are a total of 96 frequency pairs allowed, as shown in Fig. 2. By example, the RBU 12 may transmit in the 3' frequency band and receive in the 3 frequency band, and the SU 14 transmits in the 3 frequency band and receives in the 3' frequency band.

The RBU 12 can support 128 simultaneous 34 Kbps channels using the 2.72 MHz bandwidth giving it a spectral efficiency of 1.6 bits/Hz. Of this total capacity, 8 channels are used by the FWS 10 and an additional 2 Kbps per channel is system overhead. Thus the effective traffic carrying capacity is 120 channels at 32 Kbps.

The spectral efficiency of the FWS 10 is three to five times that of conventional CDMA systems primarily because the FWS 10 employs bi-directional Synchronous CDMA. Competing systems, including those based on IS-95, are asynchronous or synchronous only in one direction. The bi-directional synchronicity permits the FWS 10 to use near orthogonal spreading codes and gain maximum possible data carrying capacity.

Radio emissions lose energy as they travel in air over long distances. In order to ensure that the received signal energy from a distant subscriber is not completely overwhelmed by that of a near subscriber, the RBU 12 controls the power level of the SUs 14. In the preferred embodiment only the reverse channel power (from SU 14 to

the RBU 12) is controlled by the RBU 12. The power control is primarily established at SU 14 initialization.

Subsequent power adjustments are infrequent and are made in response to transient environmental conditions. The closed loop power control is implemented by comparing against a desired power level and making incremental adjustments until the desired level is achieved.

The forward channel power control is not needed since each SU 14 receives its entire signal at only one level. The RBU 12 merely needs to ensure that the received signal strength by the farthest SU 14 is sufficient for its application.

It is not always desirable to have an extended range. In a dense urban or even a suburban setting, one needs to deploy the system in a cellular architecture as depicted below. To reduce interference between sectors and between cells in such a deployment, the range of the RBU is limited overall as well as selectively in specific directions. Such range control may be accomplished using a directional master antenna 12b at the RBU 12, as well by controlling overall RBU power.

When one of the SUs 14 detects an off-hook (the user has picked up the phone), it transmits an outgoing call request on one of six reverse synchronous side channels in a Slotted ALOHA fashion. The side channel is chosen at random. The RBU 12 processes the request and, providing an active channel is available, sends an outgoing call reply to the SU 14 which contains the active channel codes (both forward and reverse). In the meantime, the RBU 12 begins to transmit forward side channel data on the newly activated channel and at a given time, begin to transmit the active call data. The SU 14, which is listening to the forward side channel, receives the active channel assignment and

switches at a superframe boundary to the active codes. The SU 14 then begins to receive the side channel data and then the active call data.

When an incoming call is received by the NIU 13 for one of the SUs 14 in the local loop, the RBU 14 is notified over the E1 link. The RBU 12 first checks to determine if the intended SU 14 is busy. If not, the RBU 14 sends a message to the SU 14 on the forward side channel, the message containing the active channel codes. The call processing then continues in the same manner as the outgoing call processing discussed above.

If all channels are busy and the NIU 13 receives an incoming call for a non-busy SU 14, it provides a subscriber busy tone to the caller unless the called SU has priority inbound access (such as a hospital, fire station, or police), in which case the NIU 13 instructs the RBU 12 to drop the least priority call to free up a channel for the called SU 14. Similarly, if an SU 14 initiates a request for service and no traffic channels are open, then the RBU 12 provides the dial tone on a temporary traffic channel and receives the dialed number. If the dialed number is an emergency number the RBU 12 drops a least priority call to free up a traffic channel and connects the free channel to the SU 14. If the called number is not an emergency number then the SU 14 is provided a special busy tone indicating a "wait for service" condition.

Reference is now made to Fig. 3 for illustrating the RBU 12 and SU 14 in greater detail.

An incoming call from the PSTN 13a passes through the NIU 13 to 64 Kbps per channel E1 trunks 13b and then to a RBU-resident E1 interface 20. The E1 interface 20 optionally performs an A-Law ADPCM algorithm for the compression of

the 64 Kbps channel to a 32 Kbps channel that is placed on a PPCM highway 21 time slot. If the A-Law ADPCM compression is bypassed, the 64 Kbps channel is split into two 32 Kbps channels and placed onto the PPCM Highway 21. In the preferred embodiment the RBU 12 can accommodate up to 128 32 Kbps channels, and each SU 14 can accommodate up to four 32 Kbps channels. The PPCM Highway 21 operates in conjunction with a frame synchronization (FrameSync) signal 20a, which represents a master timing pulse that is generated every 16 ms. All calls to and from the RBU 12 pass through the PPCM Highway 21 and the E1 interface 20. For the case of an incoming call the signal is applied to a baseband combiner (BBC) 22 and thence to a D/A converter 24 and a transmit radio frequency front-end (RFFE) 26 before being applied to the antenna 12b for transmission to the SU 14. At the SU 14 the incoming call signal is received by the antenna 14a and is applied to a receive RFFE 34, an A/D 36, demodulator 38 and a receiver 40. The SU 14 includes a subscriber line interface circuit (SLIC) 42 that couples a pulse code modulation (PCM) Highway 43 to a network termination unit (NTU) 52. In the reverse direction a call originates at the NTU 52 and passes through the SLIC 42 and PCM Highway 43 to a transmitter 44, modulator 46, D/A converter 48 and a transmit RFFE 50. The signal is applied to the SU antenna 14a and is received by the RBU antenna 12b. The received signal is applied to a receive RFFE 28, A/D converter 30, a demodulator and synchronization unit 32, and then to the PPCM Highway 21 and E1 interface 20 for connection to the PSTN 13a via one of the E1 trunks 13b and the NIU 13.

The RBU 12 controls the master timing for the entire FWS 10. Timing throughout the FWS 10 is referenced to the periodic timing pulse generated at the PPCM Highway 21, i.e., to the FrameSync signal 20a. In the FWS 10 all data is grouped into equal-sized packets referred to as frames,

which in turn are grouped into super-frames with, for example, three frames making up one super-frame.

Reference is now made to Figs. 5A and 5B for illustrating the presently preferred S-CDMA waveform generation circuitry. In the RBU 12 both data (32 Kbps) and control messages (1.5 Kbps) are multiplexed into a single bit stream (34 Kbps) using a multiplexer (MUX) 53. The data stream is rate 1/2 convolutionally encoded at block 54 and then punctured to 4/5ths (a rate 4/5 punctured trellis code) in block 56 thereby producing I and Q symbol pairs. Un-encoded SYNC words (312.5 symbols/sec, I SYNC and Q SYNC) are then inserted at the beginning of each frame in the SYNC insertion MUX 58. The resulting I/Q symbol pairs (21.25 K symbols/sec) are spread in spreaders 60A and 60B, respectively, using, in accordance with an aspect of this invention, identical pn codes for both I and Q. The resulting chip waveform (2.72 M chips/sec) is then presented to the D/A converter 24 and transmit RFFE 26 where the waveform is upconverted to the transmit frequency.

The waveform is identical for both the Forward (downlink) and Reverse (uplink) channels, except that in the forward direction every third sync word is inverted. The inverted sync word enables the SU 14 to determine where superframe boundaries occur. In the reverse direction the sync words are not inverted, as the RBU 12 already has knowledge of where the superframe boundaries occur. The reverse channel is, however, superframe synchronous so that the side channels can operate using a slotted ALOHA multiple access protocol. The reverse channel side channel bursts always begin and end on superframe boundaries.

The RF receiver of Fig. 5B downconverts the received signal to baseband. The baseband signal is despread in

despreaders 62A and 62B, again using identical pn codes, and accumulated in accumulators 64A and 64B for a symbol period, resulting in I and Q soft symbol decisions. The I/Q soft decisions are presented to a SYNC detection and removal circuit block 66. This circuitry of block 66 generates a Frame synchronization signal that is used by a depuncture block 68 and a Viterbi decoder 70 for frame synchronization. The I/Q soft decisions are presented to the depuncture block 68 where punctured data is reinserted. The I/Q output of depuncture block 68 is input to the Viterbi decoder 70 which accepts I/Q symbols and outputs received Data and Control. From the Frame synchronization signal, a Control Frame synchronization signal is generated by block 72. This signal is used by demultiplexer (DEMUX) 74 to separate the Data from the Control messages.

By using the same pn codes for both the I and Q channels the capacity of the FWS 10 is doubled when compared to a system that uses separate I and Q pn codes.

Referring to Fig. 4, Data and Control messages are contained in 16 ms frames 80. Each 16 ms frame 80 is comprised of four, 16-byte blocks or fields of data 80A and three 1-byte control (CTRL) blocks or fields 80B. A single control message frame 82 is comprised of a plurality of one-byte fields, specifically a control message header field which can be used to identify a type of control message, two control data fields, and two CRC (XOR encryption) data integrity fields. The number of fields may be varied. The control message frame 82 requires more than one data frame 80 to be completely transmitted. Each data frame 80 begins with a 1-byte synchronization (SYNC) word 80B. The SYNC word 80C is not encoded. Rather, it is inserted at the symbol rate in the SYNC insertion MUX 58, after puncturing, and is removed in the SYNC detection and removal block 66 before depuncturing and decoding. The

SYNC word 80C is used by the RBU receiver to obtain frame synchronization. The SYNC word 80C is also used by the Viterbi decoder 70 to resolve any I/Q phase ambiguity resulting from the up and down conversion at RF.

As was discussed earlier, in conventional approaches the control messages are put on a queue for earliest transmission, and the frame structures are typically designed to transmit all control for a particular frame in a single block either at the beginning or end of the frame. However, this approach adds a delay to transmit all control for a particular frame in a single block either at the beginning or end of the frame, and thus adds delay to messages and telephony data at the receiver.

In accordance with the frame structure shown in Fig. 4 a control message does not have to be delayed by an entire frame. Instead, it can be transmitted in the first of three 1 byte control blocks that are interspersed with the frame data fields 80A, resulting in a significant reduction in latency. This also has the effect of minimizing the delay experienced by the telephony data. That is, by sending the control messages in "packets" within the data frame 80, the telephony data experiences less delay. This feature enables the FWS 10 to implement tighter control loops as well as to decrease the time required to establish and tear-down channels.

While the invention has been particularly shown and described with respect to preferred embodiments thereof, it will be understood by those skilled in the art that changes in form and details may be made therein without departing from the scope and spirit of the invention.

CLAIMS

What is claimed is:

1. A method for transmitting information in a Code Division Multiple Access communication system, comprising steps of:

multiplexing data and control information into a data stream;

encoding the data stream to form a stream of encoded I/Q symbol pairs;

inserting synchronization information into the stream of encoded I/Q symbol pairs; and

spreading the encoded I/Q symbol pairs and the inserted synchronization information using a same pseudonoise (pn) spreading code prior to transmission as a frame.

2. A method as in claim 1, wherein the step of multiplexing forms a data stream having data fields comprised of a plurality of data bytes separated by control message fields each comprised of a single byte of a control message frame.

3. A method as in claim 2, wherein the control message frame is comprised of a control message header field, a plurality of control data fields, and a plurality of data integrity fields.

4. A method as in claim 1, wherein the frame is comprised of an unencoded synchronization field followed by a plurality of data fields each comprised of a plurality of

data bytes, individual ones of said plurality of data fields being separated by a control message field each of which is comprised of a single byte of a multi-byte control message frame.

5. A method as in claim 1, wherein the step of encoding includes steps of:

rate 1/2 convolutionally encoding the data stream to form an I channel and a Q channel; and

rate 4/5 punctured trellis coding the I and Q channels.

6. A method for transmitting information in a Code Division Multiple Access communication system, comprising steps of:

multiplexing data and control information into a data frame having data fields comprised of a plurality of data bytes separated by control message fields each comprised of a single byte of a multi-byte control message frame;

encoding the data frame;

inserting an unencoded synchronization field into the data frame;

spreading the data frame using a spreading code; and

transmitting the spread data frame to a receiver.

7. A method as in claim 6, and further comprising steps of:

receiving and despreading the transmitted data frame;

synchronizing to the synchronization field;

decoding the data frame; and

demultiplexing the data fields from the control message fields.

8. A method as in claim 7, wherein the control message frame includes a control message header field, a plurality of control data fields, and a plurality of data integrity fields.

9. A method as in claim 6, wherein the step of encoding includes steps of:

rate 1/2 convolutionally encoding the data frame to form an I channel and a Q channel; and

rate 4/5 punctured trellis coding the I and Q channels.

10. A synchronous CDMA fixed wireless system comprised of a radio base unit (RBU) coupled to a telecommunications network and to a plurality of subscriber units (SUs) that communicate over CDMA radio channels, said RBU comprising:

a first multiplexer for multiplexing data and control information intended for one SU into a data frame having data fields comprised of a plurality of data bytes separated by control message fields each comprised of a single byte of a multi-byte control message frame;

an encoder for encoding the data frame and forming

encoded I/Q symbol pairs;

a second multiplexer for inserting unencoded I/Q symbol pairs of a synchronization field into the encoded I/Q symbol pairs to form a multiplexed I/Q symbol pairs stream;

a spreader for spreading the multiplexed I/Q symbol pairs stream using one pn spreading code; and

a transmitter for transmitting the spread multiplexed I/Q symbol pairs stream as a frame to the intended SU.

11. A system as in claim 10, wherein the said encoder comprises:

a rate 1/2 convolutional encoder; and

a rate 4/5 punctured trellis coder.

12. A system as in claim 10, wherein said transmitted frame is comprised of an unencoded synchronization field followed by a plurality of data fields each comprised of a plurality of data bytes, individual ones of said plurality of data fields being separated by a control message field each of which is comprised of a single byte of a multi-byte control message frame.

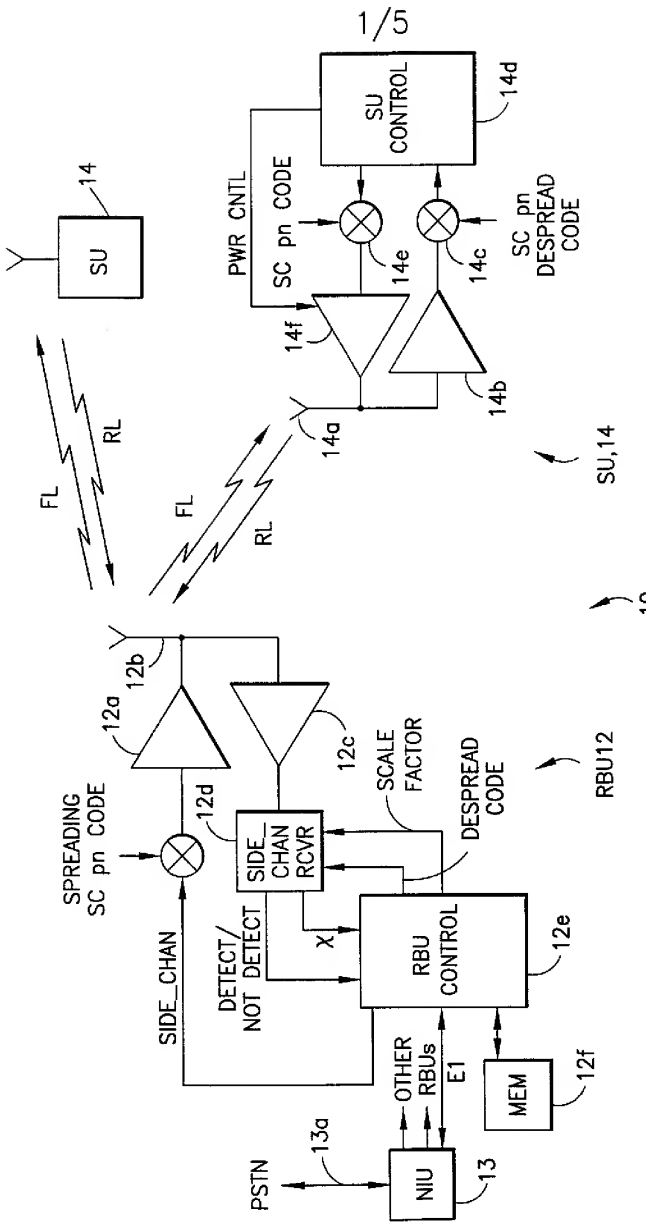

SU
14
FL
RL
FL
RL
14a
14f
14e
14c
14b
PWR CNTL
SC pn CODE
SC pn DESPREAD CODE
SU CONTROL
14d
SU,14
10
12a
12b
12c
12d
SPREADING SC pn CODE
SIDE_CHAN
SIDE CHAN RCVR
SCALE FACTOR
DESPREAD CODE
RBU12
DETECT/ NOT DETECT
X
RBU CONTROL
12e
OTHER RBUs
E1
MEM
12f
PSTN
13a
NIU
13

FIG.1

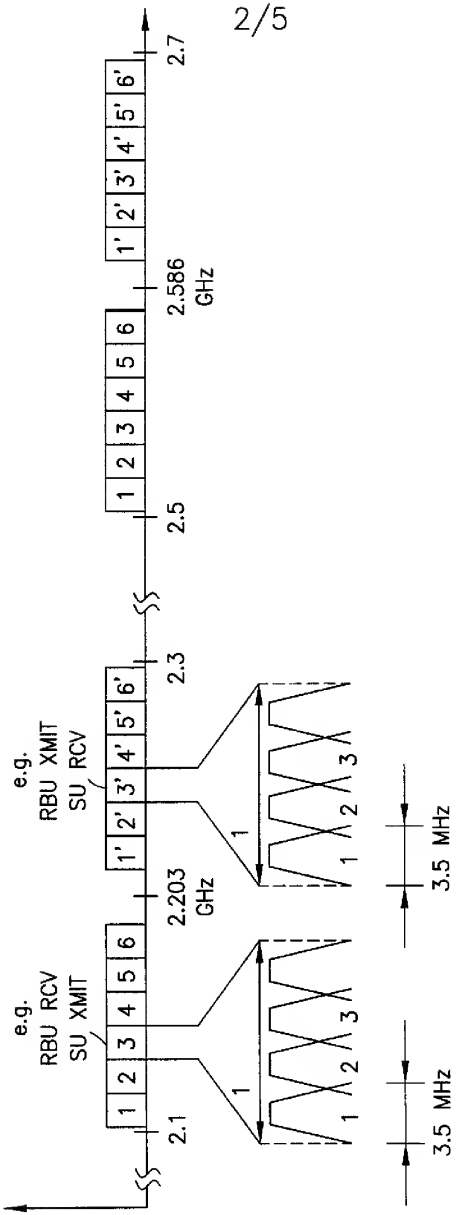

e.g.
RBU RCV
SU XMIT
e.g.
RBU XMIT
SU RCV
1 2 3 4 5 6
1' 2' 3' 4' 5' 6'
2.1
2.203 GHz
2.3
2.5
2.586 GHz
2.7
3.5 MHz
3.5 MHz

FIG.2

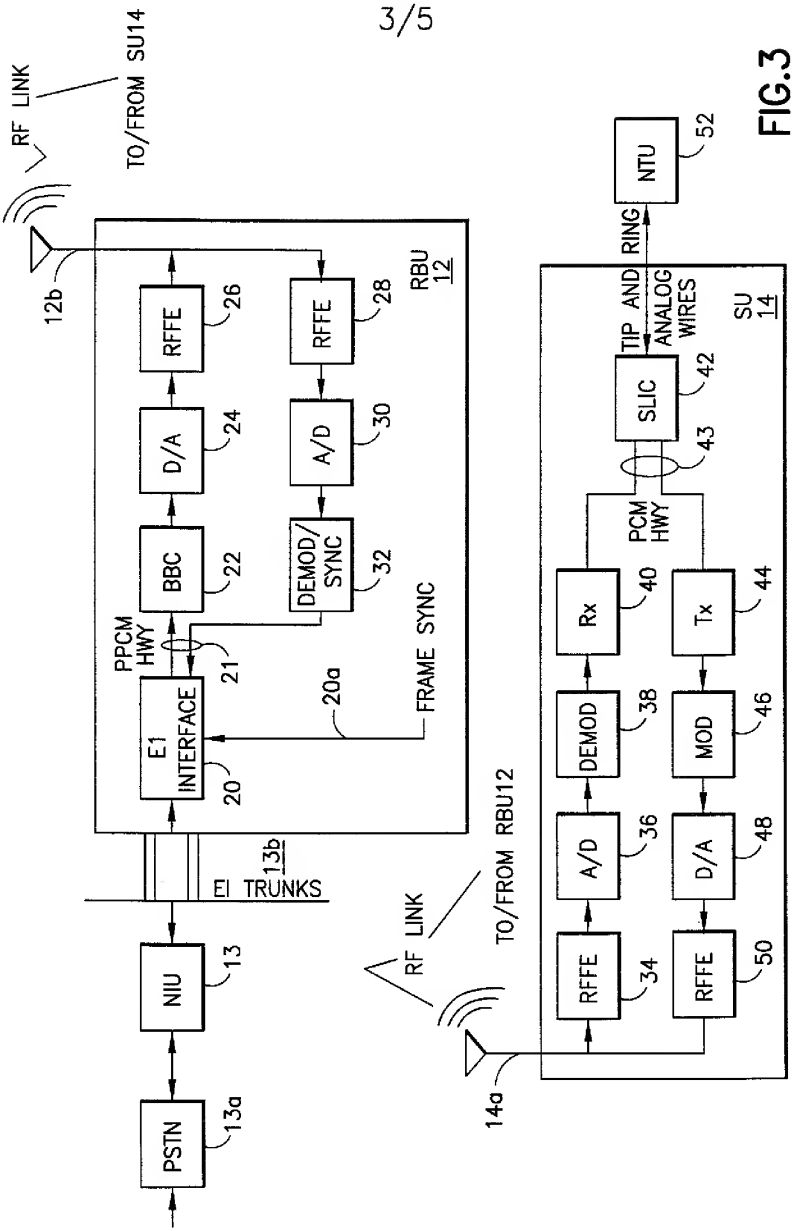

RF LINK
TO/FROM SU14
12b
RBU 12
RFFE 26
D/A 24
BBC 22
PPCM HWY
21
E1 INTERFACE 20
20a
FRAME SYNC
RFFE 28
A/D 30
DEMOD/ SYNC 32
13b
E1 TRUNKS
NIU 13
PSTN 13a
RF LINK
TO/FROM RBU12
14a
RFFE 34
A/D 36
DEMOD 38
Rx 40
PCM HWY
43
SLIC 42
TIP AND RING ANALOG WIRES
SU 14
NTU 52
RFFE 50
D/A 48
MOD 46
Tx 44

FIG.3

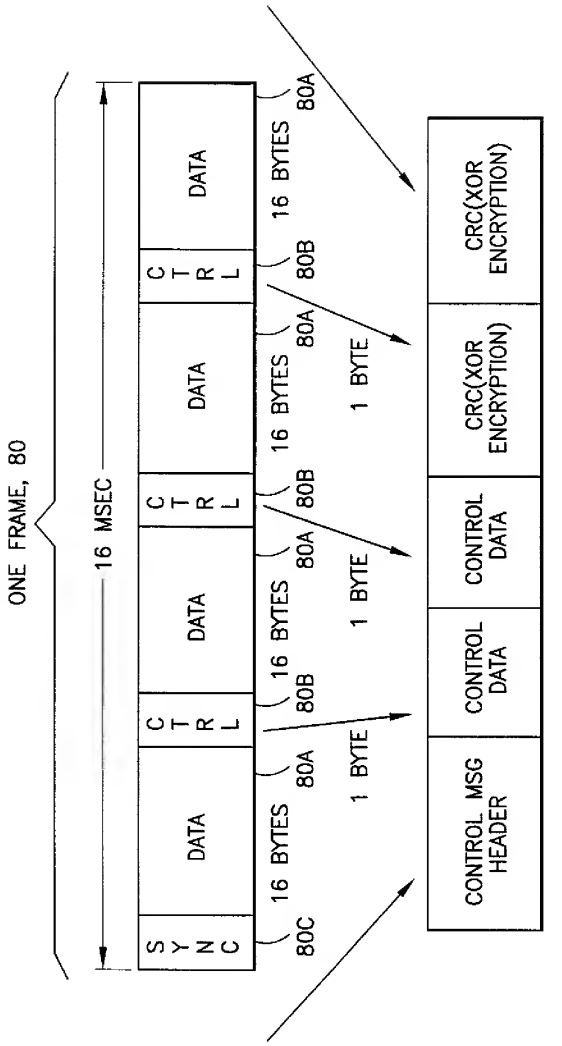

ONE FRAME, 80
16 MSEC
SYNC
DATA
CTRL
16 BYTES
80C
80A
80B
1 BYTE
CONTROL MSG HEADER
CONTROL DATA
CRC(XOR ENCRYPTION)
CONTROL MESSAGE FRAME, 82

FIG.4

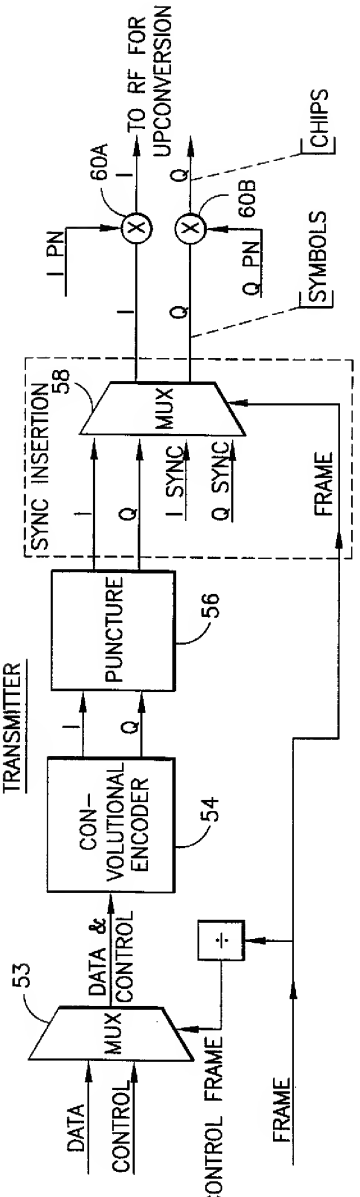

TRANSMITTER
DATA
CONTROL
53
MUX
DATA & CONTROL
CONTROL FRAME
÷
FRAME
CON-VOLUTIONAL ENCODER
54
I
Q
PUNCTURE
56
SYNC INSERTION
58
MUX
I SYNC
Q SYNC
FRAME
I PN
Q PN
60A
60B
SYMBOLS
CHIPS
TO RF FOR UPCONVERSION

FIG.5A

RECEIVER
CHIPS
SYMBOLS
SYMBOL_TIME
I PN
Q PN
62A
62B
Σ
64A
64B
SYNC DETECTION AND REMOVAL FIFO
66
FRAME
DE-PUNCTURE
68
VITERBI DECODER
70
÷
72
DATA & CONTROL
DE-MUX
74
DATA
CONTROL
CONTROL FRAME

FIG.5B

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/24472

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 11/10; H04J 3/24; H04L 1/02; H04B 15/00; H04K 1/00

US CL : Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/335, 342, 206, 522, 474; 371/43.1, 43.2, 43.4, 52; 375/200, 206, 208, 265, 244, 316

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, WEST, IEEE

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,357,541 A (COWART) 18 October 1994, col. 3, lines 29-60, col. 17, lines 24-34	1-12
Y	US 5,396,518 A (HOW) 07 March 1995, col. 3, lines 5-69, col.4, lines 1-68, col. 5, lines 1-29	1-12
Y	US 5,293,379 A (CARR) 08 March 1994, col. 5, lines 27-36, col. 2, lines 21-43	2-4
Y	US 5,844,922 A (WOLF et al) 01 December 1998, col. 3, lines 14-63, col. 4, lines 28-66	5-12

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 17 JANUARY 1999	Date of mailing of the international search report 02 APR 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 308-6743	Authorized officer AFSAR M. QURESHI Telephone No. (703) 308-8542

Form PCT/ISA/210 (second sheet)(July 1992) *

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/24472

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,396,518A [HOW] 07 March 1995, col. 3, lines 5-69, col. 4, lines 1-68, col. 5, lines 1-29	1-12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/24472

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

370/335, 342, 206, 522, 474; 371/43.1, 43.2, 43.4, 52; 375/200, 206, 208, 265, 244, 316

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04Q 7/22 — A2

(11) International Publication Number: **WO 99/59355**

(43) International Publication Date: 18 November 1999 (18.11.99)

(21) International Application Number: PCT/FI99/00413

(22) International Filing Date: 12 May 1999 (12.05.99)

(30) Priority Data:
981065 13 May 1998 (13.05.98) FI

(71) Applicant *(for all designated States except US)*: NOKIA NETWORKS OY [FI/FI]; Keilalahdentie 4, FIN–02150 Espoo (FI).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: MUHONEN, Ahti [FI/FI]; Itälahdenkatu 5 B 37, FIN–00210 Helsinki (FI). HAUMONT, Serge [FR/FI]; Riistavuorenkuja 3 B 10, FIN–00320 Helsinki (FI). ROOKE, Michael [GB/FI]; Kyyhkysmäki 4 D 32, FIN–02600 Espoo (FI).

(74) Agent: KOLSTER OY AB; Iso Roobertinkatu 23, P.O. Box 148, FIN–00121 Helsinki (FI).

(81) Designated States: AE, AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

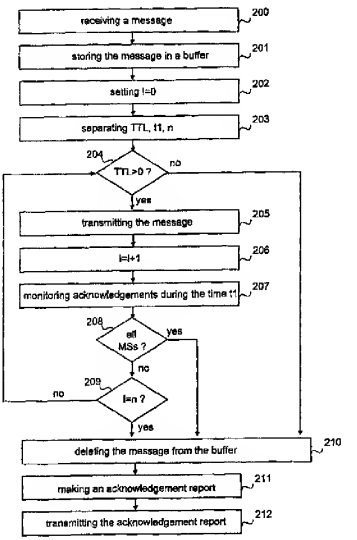
Published

In English translation (filed in Finnish).
Without international search report and to be republished upon receipt of that report.

(54) Title: POINT–TO–MULTIPOINT TRANSMISSION IN A MOBILE COMMUNICATION SYSTEM

(57) Abstract

A method, a system and a network element for controlling the transmission of a message to be transmitted point–to–multipoint in a mobile communication system. In order to take the topicality of the content of the message to be transmitted point–to–multipoint into account, a life time is determined for the message in the method and the message waiting to be transmitted is deleted from the buffer (210) in response to the expiry of the life time.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

POINT-TO-MULTIPOINT TRANSMISSION IN A MOBILE COMMUNICATION SYSTEM

BACKGROUND OF THE INVENTION

The invention relates to point-to-multipoint transmissions in a mobile communication system and, more particularly, to point-to-multipoint transmissions which have to be acknowledged.

Mobile communication systems have been developed in order to free people from fixed telephone terminals without hindering their reachability. Coinciding with the increased use of various data transmission services at offices, a plurality of data services has also appeared in mobile communication systems. Mobile networks for their part provide a user with an efficient access network for mobile data transmission, the network giving the user access to the actual data networks. On this account, various new forms of data services are being designed for the current and future mobile communication networks. Digital mobile communication systems, like the Global System for Mobile Communication GSM, are particularly suitable for supporting mobile data transmission.

The General Packet Radio Service GPRS is a new service in the GSM system and one of the objects of GSM Phase 2+ standardization at ETSI (European Telecommunication Standard Institute). The GPRS allows packet data transmission to be established between mobile data terminals and external data networks, with the GSM network functioning as an access network. One of the requirements set for the GPRS is that it must interwork with different types of external data networks, such as the Internet or the X.25. networks. In other words, the GPRS and the GSM network should be able to serve all users, irrespective of which type of data networks the users wish to enter through the GSM network. This means that the GSM network and the GPRS must support and process various types of network addressing and data packet formats. The processing of data packets also comprises their routing in a packet radio network. Further, users should be able to roam from the GPRS home network to another GPRS network, whose operator backbone network may support a protocol (e.g. CLNP) different from that of the home network (e.g. X.25). The GPRS network architecture is illustrated in Figure 1.

The GPRS supports both point-to-point and point-to-multipoint transmissions. The aim of a point-to-multipoint transmission is to allow a sender to transmit data to recipients in a destination area by using one service

request. The term 'data' refers in this application to any information to be conveyed in a digital telecommunication system. The information may comprise digitized speech, inter-computer data communication, telefax data, short program code segments etc. The destination area is a geographical area determined by the sender. The destination area is determined either in the service request or when the starting of a point-to-multipoint transmission is notified.

To control point-to-multipoint transmissions the GPRS network typically comprises a Point-To-Multipoint Service Centre PTM-SC, which is an essential element in the point-to-multipoint service. The centre receives service requests from a Service Requester and transmits the service to its service area via the Serving GPRS Support Node SGSN. Actual point-to-multipoint services supported by the GPRS are Point-to-Multipoint Multicast PTM-M and Point-To-Multipoint Group call PTM-G. In the GPRS system, the term 'group' refers to several mobile stations which have registered with the same International Mobile Group Identifier IMGI. Groups can either be open or closed. An open group can be joined by anyone, whereas a closed group includes only the subscribers who have been defined to belong to the group in the service centre PTM-SC. Besides the actual point-to-multipoint transmissions, the GPRS supports IP Multicast IP-M according to the Internet protocol.

A PTM multicast PTM-M is broadcast in all the cells belonging to the destination area. It can be directed to all mobile stations in the cells or to mobile stations belonging to a certain group. A PTM multicast is unidirectional, non-encrypted and unreliable. Thus, anyone can listen to the transmission and the sender cannot know, whether the receiver/s has/have received the message. A message to be transmitted as a PTM multicast includes scheduling information. Scheduling information comprises the starting time, the end time and the frequency rate of the transmission. If the starting time zero is given, it deals with a real time transmission. Real time means that a message received from the service requester is transferred as quickly as possible. Transmission rate and transmission time delay vary depending on the loading of the network elements. If each piece of scheduling information is marked with zero, it deals with a real time single transmission. If the starting time is other than zero, it deals with a delayed transmission. On the basis of the time difference between the starting and end time and of the frequency

rate, the service centre PTM-SC calculates the number of transmission repetitions and the time slot between the repetitions. By using this information, PTM-SC controls the transmissions of the message. The end time is only used in calculating the control information of the above mentioned transmissions.

A PTM group call PTM-G is transmitted in the cells of the destination area which include at least one mobile station registered to the group. Only a mobile station registered to the group in the area of a serving support node SGSN can receive messages of a group call and decode the encryption. Thus, the network is aware of the location of the registered mobile stations. A PTM group call can be transmitted as a broadcast, a point-to-point transmission or as a combination of these. A group call is always individualised by the mobile group identity IMGI. In a PTM group call, a transmission is either uni-, bi- or multidirectional, encrypted and reliable. Usually the messages of a PTM group call are transferred in real time. It is also possible to employ a delayed transmission and/or repeated transmissions as in the PTM multicast. Since a PTM group call is reliable, at least a broadcast group call must be acknowledged. In case of a negative acknowledgement, a mobile station transmits the acknowledgement only if it notices that it has not received the previous PTM message or messages. In such a case, the service centre transmits the missing messages to it. In case of a positive acknowledgement, each PTM message is acknowledged individually. A positive acknowledgement is especially applicable to cases in which the reliability requirements are strict. In both manners of acknowledging, each acknowledgement transmitted by a mobile station is conveyed via the serving support node SGSN to the service centre, which decides on the following actions on the basis of the acknowledgements. At the end of the PTM group call, the service centre PTM-SC transmits a report to the service requester.

On the basis of what is described above, a problem arises that a point-to-multipoint message can only be transmitted after the content of the message has already gone out of date. This is the case particularly in the transmissions which have to be repeated and transmitted as scheduled. On the other hand, a group message which has to be acknowledged cannot be delivered to the mobile stations which have not received it at the time of the actual transmission, although the mobile stations arrived at the destination area during the time the content of the message has not yet gone out of date.

BRIEF DESCRIPTION OF THE INVENTION

It is thus the object of the invention to provide a method and an apparatus implementing the method in such a way that the above problems can be eliminated. The objects of the invention are achieved by a method, which is characterized by determining a life time for a message, and deleting the message from a buffer in response to the expiry of the life time.

The term 'buffer' refers herein to a memory, in which the message is temporarily stored to wait for forwarding and/or successive transmissions.

The invention also relates to a mobile communication system, to which the method of the invention can be applied. The system comprising at least one service centre PTM-SC to transmit a message as a point-to-multipoint transmission and at least one network element SGSN via which the message is transmitted to cells belonging to a destination area is characterized in that the service centre PTM-SC is arranged to determine the remaining life time of the message and to check before transmitting the message, whether there is life time left and to transmit the message only if there is still life time left.

The invention further relates to a network element of a mobile communication network, by which network element the method of the invention can be applied. The network element is characterized in that it comprises means for determining the remaining life time of a message to be transmitted point-to-multipoint, and means for transmitting said message according to the scheduling of the message, if there is still life time left.

The invention is based on giving a message a precise life time. As the life time expires, the message will not be transmitted anymore. At its simplest, this is ensured by deleting the message from the transmission buffer. This provides the advantage that the service requester may transmit fairly short-lived information as a point-to-multipoint transmission, because the requester knows that everyone receives the information before it goes out of date. A dated message is deleted from the group of messages to be transmitted, even if it had not been transmitted at all because of the great transmission delays. This saves the network resources and the recipients do not receive unnecessary messages.

In a preferred embodiment of the invention relating to group calls transmitted as calls to be acknowledged, it is checked whether a predetermined part of the group members has acknowledged the message,

and if it has, the message will not be transmitted anymore. This provides the advantage that the message transmitted as a group call will not be unnecessarily retransmitted. This saves the network from unnecessary loading.

In a preferred embodiment of the invention, in which a message is received from another network element, the acknowledgement transmitted to it includes information on the group members who have received the message. This provides the advantage that the loading of the network decreases substantially. In known prior art solutions, acknowledgements are transmitted individually to the service centre PTM-SC. The acknowledgements differ from each other only in respect of the subscriber identification data. When using positive acknowledgements in particular, the loading of the network decreases. If e.g. the support node SGSN succeeds in transmitting a PTM group call to x subscribers, it only conveys one acknowledgement, instead of x acknowledgements, to the service centre PTM-SC.

In a preferred embodiment of the invention, the service centre attempts during the whole life time of the message to transmit the message to those group members who become reachable during the life time of the message and have not yet received the message. This provides the advantage that a long life time of a message allows the service requester to ensure that as many group members as possible get the important message. An effort is not, however, made to resend the message to those who have already received it. This saves the network resources.

The preferred embodiments of the method, system and network element of the invention are disclosed in the attached dependent claims.

LIST OF FIGURES

In the following the invention will be described in greater detail in connection with the preferred embodiments, with reference to the attached drawings, in which

Figure 1 shows a block diagram of some elements in a packet radio system of the invention,

Figure 2 shows a flow chart of an operation in a serving support node SGSN according to a first preferred embodiment of the invention, and

Figure 3 shows a flow chart of an operation in a service centre PTM-SC according to the first preferred embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following, the preferred embodiments of the invention will be described by means of GPRS packet radio networks yet without restricting the invention to such a specific packet radio system. The invention is applicable to all mobile communication systems in which point-to-multipoint transmissions are possible, e.g. to the third-generation mobile communication systems UMTS (Universal Mobile Telecommunication System) and IMT-2000 (International Mobile Telecommunication 2000) which are under development. It is to be noticed that the packet radio network only provides a physical connection between the PTM service centre and the service recipient, and the exact operation and structure of the network have no substantial meaning for the invention. The specifications of mobile communication systems in general and of the GPRS system in particular evolve fast. Various functionalities of the network elements may change. Therefore, all terms and expressions should be interpreted as widely as possible, and they are intended to describe and not to limit the invention.

Figure 1 shows an example of a GPRS packet radio network PLMN. A GPRS operational environment 1 comprises one or more subnetwork service areas, which are connected to each other by an Intra-GPRS Backbone Network 2. A subnetwork comprises a set of packet data service nodes SN, which are herein called serving GPRS support nodes SGSN, each of which is connected to a GSM mobile communication network 3, and typically to its base station systems BSS, in such a way that it is able to provide mobile stations MS with a packet data service via various base stations, i.e. cells. A mobile station refers herein to the entity of a mobile communication network subscriber and a data terminal equipment. The mobile communication network 3 between them provides packet-switched data transmission between the support node and the mobile stations.

On the network side, each support node SGSN controls certain functions of the packet radio service in the area of one or more cells in a cellular packet radio network. Such functions are e.g. logging of the mobile stations MS in and out of the system, updating routing zones of the mobile

stations MS and routing of data packets to their correct destinations. The mobile station MS located in the cell communicates through the mobile communication network with the support node SGSN that constitutes the service area for the cell. The functions of the serving support node SGSN according to the first preferred embodiment of the invention are described in more detail later in connection with Figure 2.

The different subnetworks in turn are connected to an external data network 4, e.g. to a packet switched public data network PSPDN, the Internet network or to the integrated services digital network ISDN, via specific gateway GPRS support nodes GGSN. Thus, the GPRS provides packet data transmission between mobile data terminal equipment and external data networks with the GSM network 3 serving as an access network. The different mobile communication networks are connected to each other by an Inter-GPRS Backbone Network 5. The GPRS operational environment 1 comprises a Border Gateway BG situated on the connection between the mobile communication networks. The GPRS subscriber data and the routing information are stored in the home location register HLR of the GSM network.

To control point-to-multipoint transmissions the GPRS network typically comprises a point-to-multipoint service centre PTM-SC. The service centre PTM-SC is the central element in the point-to-multipoint service and it is responsible for the geographical routing of messages. It receives service requests from the service requester SR and transmits the service via the support node/s SGSN of its service area. In other words, it takes care of the scheduling, transmission and retransmission of messages according to given parameters. The functions of the service centre according to the first preferred embodiment of the invention are described in more detail in connection with Figure 3. Some of the service centre functions can be decentralized into other network elements, e.g. into the support node SGSN which can take care of at least some of the transmissions in the system of the invention. So far, GPRS specifications do not determine how a PTM service centre is connected to a network. Figure 1 shows one alternative, in which the PTM service centre is connected to the internal backbone network 2.

In the system of the invention, the service requester SR is not limited in any way. The service requester can thus be an independent service provider transmitting its service request via other networks 4. The service requester SR can also have a direct connection to the service centre PTM-SC

located in the network, as shown in the example of Figure 1. The service requester can also be a network element or a terminal, whose service request is forwarded to the service centre PTM-SC. Further, it can be some other service centre PTM-SC.

To implement the invention, any equipment changes do not need to be made to the network structure described above. The service centre PTM-SC and the serving support nodes comprise processors, timers and memory, which can be utilized in buffering the message and observing the life time. Al the changes needed for implementing the invention can instead be performed as added or updated software routines in the service centre PTM-SC and/or in the serving support node SGSN. The invention can thus be implemented relatively easily in the network elements.

Figure 2 shows the operation of a serving support node SGSN in a first preferred embodiment of the invention. In the first preferred embodiment of the invention, the serving support node is assumed to be an "intelligent" serving support node. Intelligent means that the support node itself takes care of the transmissions, selects the mode of transmission (a broadcast or a point-to-point transmission) and detects the cells which include mobile stations registered to the group and which mobile stations have registered to the group.

With reference to Figure 2, one group message is received from the service centre by the serving support node SGSN in step 200, which message is stored in a transmission buffer in step 201. The group message is a message transmitted as a group call (PTM-G). In step 202, zero is set as the number of transmissions l (l=0). The remaining life time TTL, the waiting time t1 of acknowledgements and the maximum number of transmissions n are separated from the group message in step 203. In the following, waiting time of acknowledgements is also called acknowledgement time. In the first preferred embodiment of the invention, the acknowledgement time is the same as the time slot between the transmissions. This provides the advantage that it is checked before each transmission, whether the transmission conditions will be fulfilled. In step 204 it is checked, whether the message still has life time left, i.e. whether TTL > 0. If it has, the message is transmitted in step 205 to the cells which include mobile stations registered to the group. In the first preferred embodiment, the message is transmitted to the mobile stations either as a broadcast of a cell or as a point-to-point transmission from a

serving support node to a mobile station depending on which alternative loads the network less. The support node calculates the loads and decides on the mode of transmission in accordance with the routing zones. Usually one cell corresponds to one routing zone.

After the transmission, the number of transmissions I is updated by increasing it by one in step 206. Thereafter, acknowledgements of the mobile stations are being monitored in the serving support node in step 207 during the acknowledgement time t1. The calculation of the acknowledgement time t1 begins at the instant of the transmission in the first preferred embodiment. If negative acknowledgements are received during this time, the missing part of the message is retransmitted in the first preferred embodiment. In some other embodiment, the missing parts of the message cannot be transmitted until in connection with the next transmission, or the service centre PTM-SC decides on their transmission on the basis of the acknowledgement report received by it. As the acknowledgement time t1 has expired, it is checked in step 208, whether all the mobile stations registered to the group in the area of the serving support node have acknowledged the message as received. This provides the advantage that the message is not transmitted unnecessarily, if everyone has already received it. Successful point-to-point transmissions are also regarded as acknowledged. If someone has not acknowledged the message, it is checked in step 209, whether the maximum number of messages has already been transmitted (I=n?). If not, it is returned to step 204, in which it is checked whether there is still life time left. In step 205, different types of transmission solutions can be made at different transmission times owing to the fact that e.g. the mobile stations that have already acknowledged the message are "forgotten" when comparing the loading caused by a broadcast and that of point-to-point transmissions.

The loop formed by steps 204 to 209 is repeated until everyone has acknowledged the message (step 208), the maximum number of transmissions is reached (step 209) or the life time of the message has expired (step 204). If one of these conditions is fulfilled already in the first cycle, the loop is left without repeating it once. After leaving the loop, the message is deleted in step 210 from the buffer of the serving support node, an acknowledgement report is made in step 211, which report is transmitted to the serving centre PTM-SC in step 212. In the first preferred embodiment, the acknowledgement report includes a list of mobile stations which have received

the message and informs of the quality of the used service. In some other embodiment, the acknowledgement report can only include one piece of this information, either the information on the mobile stations which have not acknowledged the message as received or the information on the mobile stations which reported on the missing of the message. The information can also be represented in some other way than in the form of a list, e.g. as different parameters. Sufficient information may be e.g. the percentage of the acknowledged mobile stations. Making only one acknowledgement report has the advantage that different acknowledgements do not need to be transmitted individually. This saves the network resources.

In an embodiment in which the message is deleted from the buffer as soon as the life time has expired and there still is life time left, the expiry of the acknowledgement time is awaited and only thereafter, the acknowledgement report is made. Hereby, the acknowledgement report informs of the real situation.

It was assumed above that the waiting time t1 of the acknowledgements is the same as the time slot between the successive transmissions of the message. In some other embodiment, the waiting time t1 of the acknowledgements can be e.g. three times as long as the time slot between the transmissions, or a support node specific constant, like delay. If the waiting time of the acknowledgements is a predetermined constant, of which the serving support node is aware, it does not have to be included in the message and thus separated in step 203. The same applies to the time slot between the transmissions to be repeated, too. If the time slot between the transmissions is not a constant and it is some other than the waiting time of the acknowledgements, it must be included in the scheduling information and separated from the message.

In the above, the maximum number of transmissions was restricted to n transmissions. In some embodiments this restriction is not used, whereupon n need not be separated from the message and the checking in step 209 does not need to be performed. The maximum number of transmissions can also be a constant, of which the serving support node is aware. In this case, it need not be included in the scheduling information of the message. In some embodiments, the missing of the maximum number of transmissions from the message results in giving up the checking in step 209.

Unlike above, the number of mobile stations the service aims to reach, e.g. 90 %, can further in some embodiments be given as transmission information, e.g. scheduling information, of the message. In this case, it is moved from step 208 to step 210, if 90 % of the mobile stations registered to the group in the area of the serving support node have acknowledged the message as received.

In an embodiment, the scheduling information of the message can also include information on the starting time of the first transmission. In this case, the beginning of the starting time of the transmission is awaited before the checking in step 204.

Figure 3 shows the operation of a service centre PTM-SC in the first preferred embodiment. In step 300, a group message is received in the service centre PTM-SC from a service requester, the message being stored in a buffer of the service centre PTM-SC in step 301. Thereafter, the message is scheduled in step 302. Scheduling the message means that after the scheduling, the message includes in the first preferred embodiment at least the following information: the remaining life time TTL, the maximum number of transmissions n and the time slot t1 between the transmissions. The scheduling information can be received from the service requester in the message. A portion of scheduling information or all scheduling information can be predetermined either in group specifications or in service definitions of the service requester. For example, the life time of a message can be determined to expire always at the end of the day. Part of the scheduling information can also be support node specific constants, in which case they are not added to the scheduling information in the service centre. In the first preferred embodiment, the end time of the scheduling information is used as the expiry time of the life time. This provides the advantage that any new scheduling information is not needed. In some other embodiment, the life time can also be given separately in cases when it is not determined in advance.

After the message is scheduled, it is detected in step 303 which cells of the destination area include mobile stations MS registered to the group. In the first preferred embodiment it is enough that those serving support nodes SGSN are found to which an activated group routing context exists, letting the support nodes check the cells more accurately. In some other embodiment, the service centre PTM-SC may check the cells and their mobile stations. As the locations of the mobile stations registered to the group in the

destination area are known, it is checked in step 304, whether the life time TTL still remains. If there is still life time left, the message is transmitted in step 305 to the serving support nodes on whose area there are mobile stations registered to the group. Thereafter, acknowledgement reports are waited from the serving support nodes in step 306.

After the acknowledgement report is received in step 307, the acknowledgement information is updated in step 308 by the information of the acknowledgement report. Thereafter, it is checked in step 309 in the first preferred embodiment, whether an acknowledgement has been received from all serving support nodes SGSN to which the group message was transmitted in step 305. If not, the process starts anew in step 306 where the acknowledgement reports are awaited. After the acknowledgement has been received from all serving support nodes SGSN, it is checked on the basis of the acknowledgement information in step 310, whether all the mobile stations in the group received the message. Checking all the group members instead of only the members registered to the group in the destination area enables the delivery of the message to the mobile stations registered after the actual transmission. The actual transmission refers to a transmission performed by the serving support node. If the mobile stations belonging to the group have not received the message, it is checked in step 311, whether there is still life time left for the message. If there is, the waiting time t2 is set in the first preferred embodiment in step 312. In the first preferred embodiment, the time t2 is half of the remaining life time checked in step 311, yet at least a predetermined minimum time, e.g. the acknowledgement time or the time t1 between the transmissions (t2 = max(TTL/2, t1). This provides the advantage that as the remaining life time of the message is expiring, a more intense effort is made to reach the mobile stations which have not yet received the message. In step 313, the aim is to transmit the message to the mobile stations of the destination area which have not yet received it as a point-to-point transmission between the service centre and the mobile station. If it was observed in step 314 that the message could not be transmitted to everyone, the process changes to step 315, where the expiry of the time t2 is awaited. When the time t2 expires, it is returned to step 311 where it is checked, whether there is still life time left.

The loop formed by steps 311 to 315 is repeated until either everyone has received the message or the life time of the message has

expired. After leaving the loop, the process changes to step 316 in which the message is deleted from the buffer of the service centre. A transmission report is made in step 317 and transmitted to the service requester in step 318. The transmission report may include information on the mobile stations which received or did not receive the message in order to charge the mobile stations only for the received messages, for example. Further, the transmission report can according to the prior art include information on the quality of the transmission (QoS) and other information as well.

In some other embodiments, it can be checked in step 310, whether e.g. a sufficient number of mobile stations belonging to the group or registered to the group in the destination area has acknowledged the message. It is also possible to check, which type of service the mobile station which has not acknowledged the message has ordered. If the mobile station has ordered e.g. super service, then the loop formed by steps 311 to 315 is repeated, but if it has ordered a normal service, an effort is no longer made to transmit the message from the service centre to the mobile station.

Instead of transmitting point-to-point in step 313, the message can in some other embodiment be transmitted to the serving support nodes SGSN whose area includes the mobile stations which did not receive the message.

Instead of the loop formed by steps 311 to 315, an arrangement according to short message service can be implemented, where the home location register informs the service centre PTM-SC of the now reachable mobile station in the destination area. If there still remains life time for the message, the message is transmitted to the mobile station. This feature could be incorporated only to the mobile stations whose subscribers are willing to pay for the reception of the message a bit more. It is also possible that PTM-SC checks at regular intervals during the life time of the message, whether the mobile station has registered to the group in the destination area, and if it has, transmits the message to it. From step 309 the process may also change directly to step 316. If the service request has been transmitted both to the serving support nodes and to some other service centre, the report of this service centre is awaited in step 309 as well.

In a preferred embodiment of the invention, the service centre PTM-SC is aware of which mobile stations have registered in which routing zone under which support node SGSN. In this case, the life time is checked before transmission only in the service centre PTM-SC. The service centre informs

the support node SGSN of which packet has to be broadcast in which routing zone and which packet has to be transmitted as a PTP connection to which group member. Further, the service centre informs SGSN of the group members whose acknowledgements SGSN awaits either for a certain constant period of time or for a reported period of time. SGSN takes care of the transmissions and waits for the acknowledgements according to the instructions. After the acknowledgement time has expired, the support node SGSN transmits the received acknowledgements in an acknowledgement report to the service centre PTM-SC, which decides on the following actions on the basis of the acknowledgements and the remaining life time.

The steps described above in connection with Figures 2 and 3 are not in absolute chronological order and some of the steps can be performed simultaneously or in different order than above. Between the steps, also other functions, which relate to transmitting different point-to-multipoint transmissions, can be performed. Some of the steps can also be left out or they can be performed in another network element. It is essential that the life time of the message is under observation, and that at some point of the transmission, the remaining life time is checked or it is in some other way arranged that the message whose life time has expired will not be transmitted. The invention does not in any way relate to how group routing connections are being set up, who belong and/or are allowed to belong to the group, by which algorithm the transmission mode of the messages is selected, or how the destination area and its recipients are detected. The invention is not in any way restricted to the transmission of complete messages only, but it can be as well applied to cases in which the message has to be split into smaller frames. Although the invention is described above by relating to a message to be transmitted as a group call which has to be acknowledged, the invention is not restricted only to such point-to-multipoint transmissions. It will be apparent to a person skilled in the art how the invention is applied to other group calls and multicasts.

It is to be understood that the above description and the related figures have merely been presented to illustrate the present invention. Different variations and modifications of the invention will be apparent to those skilled in the art without departing from the scope or spirit of the invention as defined in the appended claims.

CLAIMS

1. A method for controlling a point-to-multipoint transmission of a message in a mobile communication system, in which method

the message is received (200, 300),

the message is stored in a buffer of the messages to be transmitted (201, 301),

the message is scheduled (302), and

the message located in the buffer is transmitted according to the predetermined scheduling (205, 305),

characterized by

determining a life time for the message, and

deleting the message from the buffer (210, 316) in response to the expiry of the life time.

2. A method as claimed in claim 1, **characterized** by

checking before transmitting the message, whether there is life time left (204), and

if there is, transmitting the message,

if there is not, deleting the message from the buffer.

3. A method as claimed in claim 2, **characterized** by

determining an acknowledgement time for the message to be transmitted as a group call,

transmitting the message to the group members (205),

waiting for the acknowledgements of the group members during the acknowledgement time (207),

checking after the expiry of the acknowledgement time, whether a predetermined part of the group members has acknowledged the message (208), and

if it has, deleting the message from the buffer (210),

if it has not, transmitting the message located in the buffer to the group members from whom an acknowledgement has not been received.

4. A method as claimed in claim 1, 2 or 3, **characterized** by

receiving the message to be transmitted from another network element (200),

making a report on the successful transmission of the message (211) in response to deleting the message from the buffer, and

transmitting the report to said another network element (212).

5. A method as claimed in claim 1, **characterized** by

receiving the message to be transmitted as a group call in the first network element (300),

storing the message in the buffer of the first network element (301),

transmitting the message to the second network element (305),

transmitting the message from the second network element to the group members (205),

waiting for the acknowledgements of the group members in the second network element during the acknowledgement time (207) after the transmission,

making a report on the acknowledgements in the second network element (211) after the expiry of the acknowledgement time, and

transmitting the report (212) to the first network element.

6. A method as claimed in claim 5, **characterized** by

storing the message also in the buffer of the second network element (201),

deleting the message also from the buffer of the second network element (210) in response to the expiry of the life time of the message,

checking in the second network element after the expiry of the acknowledgement time, whether a predetermined part of the group members has acknowledged the message (208), and

if it has, making a report (211) on the acknowledgements and deleting the message from the buffer of the second network element (210),

if it has not, transmitting the message located in the buffer to the mobile stations from whom an acknowledgement has not been received.

7. A method as claimed in claim 6, **characterized** by

determining the maximum number of transmissions for the message in the second network element,

calculating the number of the realized transmissions (206),

checking before transmitting the message, whether the number of the realized transmissions is the same as the maximum number (209), and

if it is, making a report on the acknowledgements and deleting the message from the buffer of the second network element,

if it is not, transmitting the message located in the buffer.

8. A method as claimed in claim 6 or 7, **characterized** by giving a report on the acknowledgements, if the message has been deleted from the buffer of the second network element before transmitting.

9. A method as claimed in claim 5, 6 or 7, **characterized** by the report including the group members who acknowledged the message as received.

10. A method as claimed in claim 9, **characterized** by the first network element being arranged to transmit the message to the group members who did not acknowledge the group message, if these group members become reachable before the life time of the message expires.

11. A mobile communication system comprising at least one service centre (PTM-SC) to transmit a message as a point-to-multipoint transmission and at least one network element (SGSN) via which the message is transmitted to cells belonging to a destination area, **characterized** in that

the service centre (PTM-SC) is arranged to determine the remaining life time of the message and to check before transmitting the message, whether there is life time left and to transmit the message only if there is still life time left.

12. A mobile communication system as claimed in claim 11, **characterized** in that the network element (SGSN) is arranged to determine the remaining life time of the message and to check before transmitting the message, whether there is life time left and to transmit the message only if there is still life time left.

13. A mobile communication system as claimed in claim 11 or 12, **characterized** in that the network element (SGSN) is arranged to receive acknowledgements from the group members during a certain acknowledgement time and to transmit the information on the acknowledgements in one message to the service centre.

14. A network element (SGSN, PTM-SC) of a mobile communication network which network supports the point-to-multipoint transmission of a message,

characterized in that the network element comprises

means for determining the remaining life time of a message to be transmitted point-to-multipoint, and

means for transmitting said message according to the scheduling of the message, if there is still life time left.

15. A network element as claimed in claim 14, **characterized** in that it (SGSN, PTM-SC) also comprises

means for determining the acknowledgement time for the message to be transmitted as a multipoint group call which has to be acknowledged,

means for monitoring the acknowledgements until the acknowledgement time has expired, and

means for compiling the acknowledgements as one acknowledgement report.

16. A network element as claimed in claim 14 or 15, **characterized** in that it (SGSN, PTM-SC) comprises means for transmitting the message to be transmitted as a multipoint group call which has to be acknowledged during the life time of the message to the group members who are reachable in the destination area of the message and who have not acknowledged the message as received.

17. A network element as claimed in claim 14, 15 or 16, **characterized** in that it (SGSN, PTM-SC) comprises a processor which is arranged to carry out software routines and that said means are implemented as software routines.

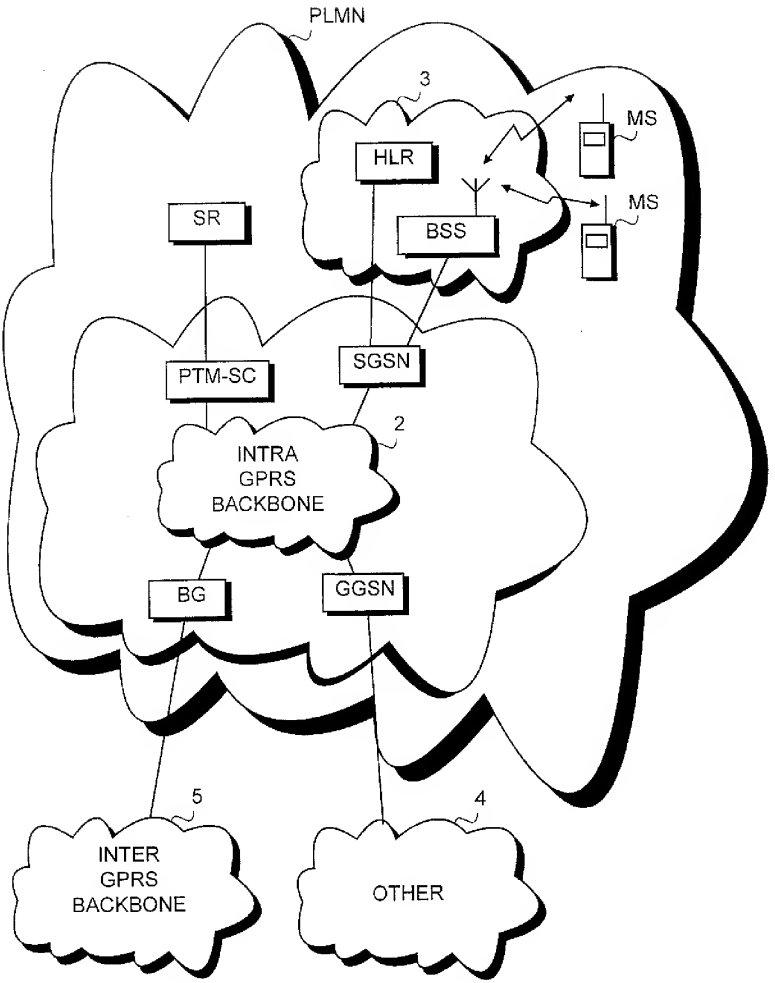

PLMN
3
HLR
MS
MS
SR
BSS
PTM-SC
SGSN
2
INTRA
GPRS
BACKBONE
BG
GGSN
5
4
INTER
GPRS
BACKBONE
OTHER

FIG.1

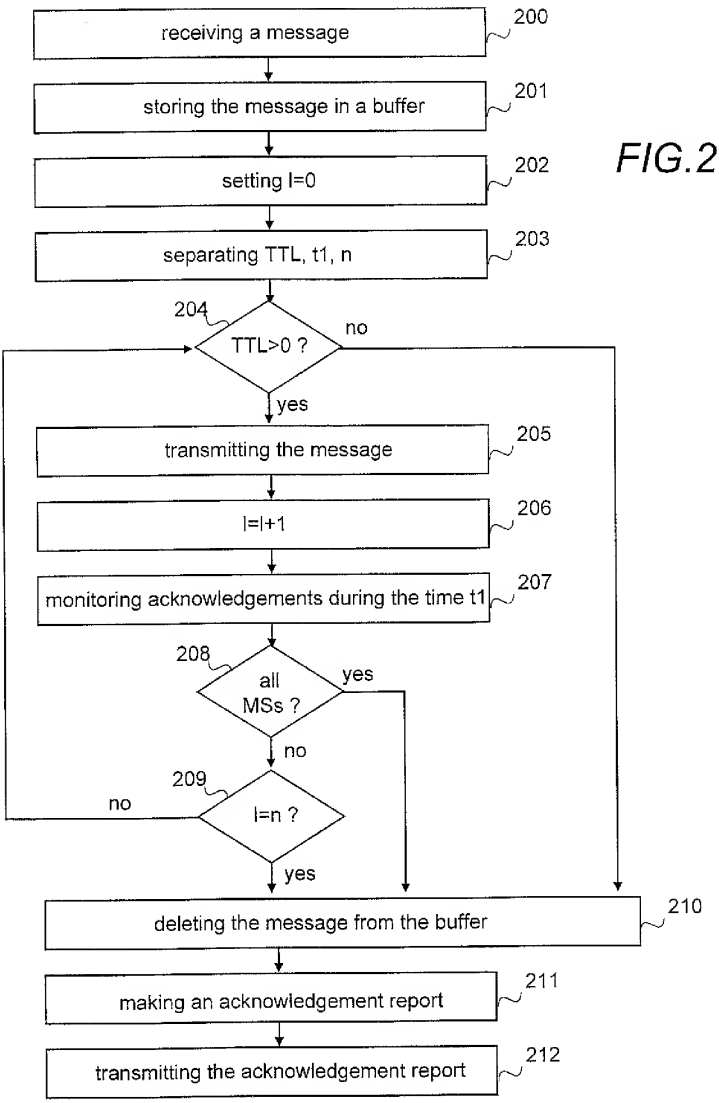

receiving a message
200
storing the message in a buffer
201
setting I=0
202
separating TTL, t1, n
203
204
TTL>0 ?
no
yes
transmitting the message
205
I=I+1
206
monitoring acknowledgements during the time t1
207
208
all MSs ?
yes
no
209
I=n ?
no
yes
deleting the message from the buffer
210
making an acknowledgement report
211
transmitting the acknowledgement report
212

FIG.2

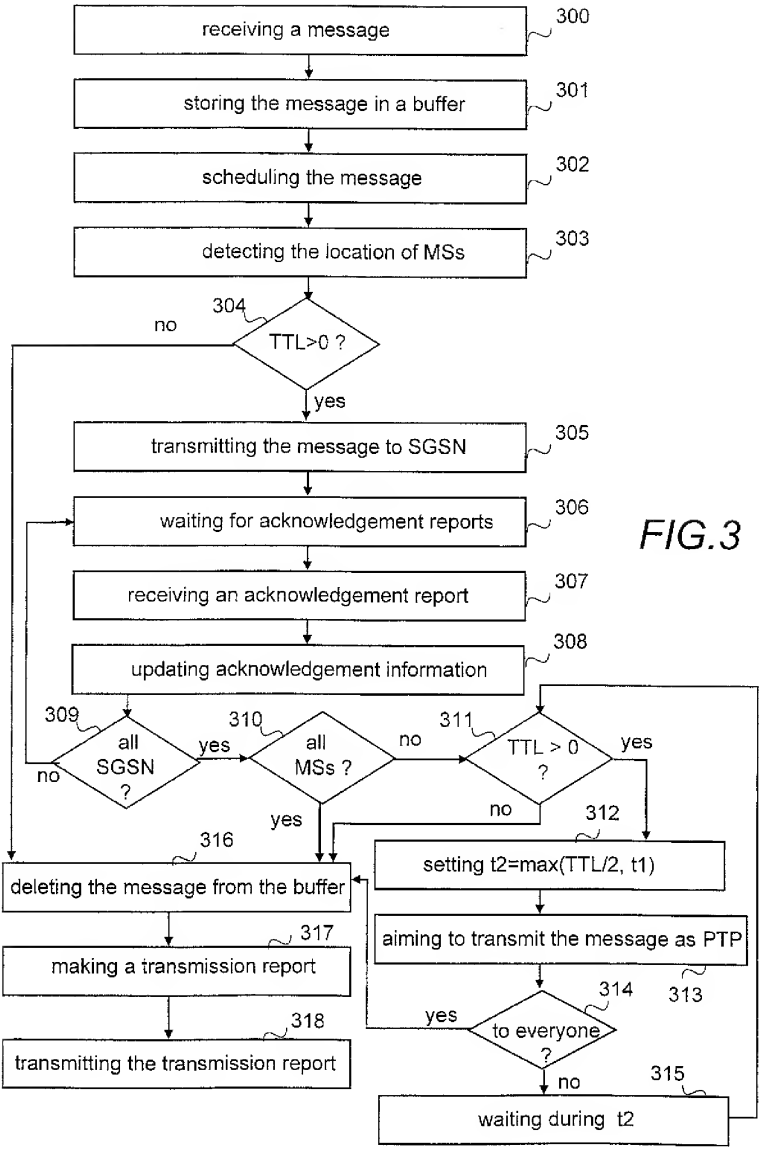

receiving a message
300
storing the message in a buffer
301
scheduling the message
302
detecting the location of MSs
303
304
TTL>0 ?
no
yes
transmitting the message to SGSN
305
waiting for acknowledgement reports
306
receiving an acknowledgement report
307
updating acknowledgement information
308
309
all SGSN ?
yes
no
310
all MSs ?
yes
no
311
TTL > 0 ?
yes
no
312
setting t2=max(TTL/2, t1)
aiming to transmit the message as PTP
313
314
to everyone ?
yes
no
315
waiting during t2
316
deleting the message from the buffer
317
making a transmission report
318
transmitting the transmission report

FIG.3

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 :
H04L 12/46, H04B 7/24

A1

(11) International Publication Number: **WO 99/62231**

(43) International Publication Date: 2 December 1999 (02.12.99)

(21) International Application Number: PCT/US99/11137

(22) International Filing Date: 20 May 1999 (20.05.99)

(30) Priority Data:

60/086,459	22 May 1998 (22.05.98)	US
09/177,751	23 October 1998 (23.10.98)	US

(81) Designated States: NO, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(71) Applicant: WINNET MCS, INC. [US/US]; 635 Vaqueros Avenue, Sunnyvale, CA 94086 (US).

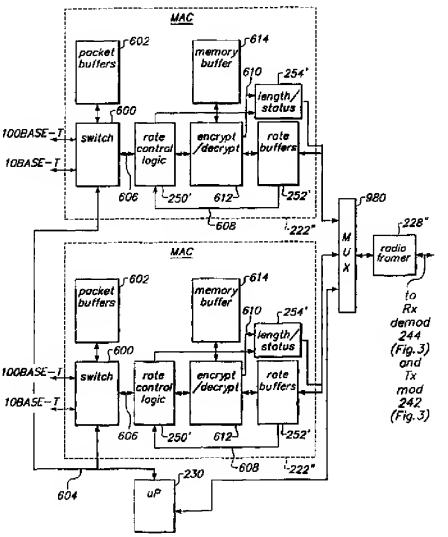
(72) Inventors: TREADAWAY, Kirk; 900 Wallace Avenue, Aptos, CA 95003 (US). HUEN, Tat; 128 Alta Vista Way, Danville, CA 94506 (US). LE NGOC, Tho; 8221 Du Mail, Anjou, Quebec H1K 1Z5 (CA).

(74) Agents: HAVERSTOCK, Thomas, B. et al.; Haverstock & Owens LLP, Suite 420, 260 Sheridan Avenue, Palo Alto, CA 94306 (US).

(54) Title: METHOD AND APPARATUS FOR A DATA TRANSMISSION OF 100 MBPS IN A TERMINAL

(57) Abstract

A method and apparatus for a data transmission rate of multiples of 100 mega-bits per second (Mbps) in a terminal for a wireless metropolitan area network. A terminal includes a first media access control unit (MAC) unit for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over a wireless link, n-1 additional MAC units for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over the wireless link, a multiplexer having n inputs, wherein each input is coupled to receive the data packets from a corresponding one of the MAC units and wherein the output of the multiplexer provides time-division multiplexed data, a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multiplexed data according to radio frames, and a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link wherein the wireless link has a maximum bandwidth capacity of at least n times 100 Mbps. Each MAC unit can include a rate control unit and a rate buffer for temporarily storing data packets received by the corresponding MAC unit prior to providing them to a corresponding one of the inputs of the multiplexer. Each MAC unit can include a corresponding layer-two or layer-three switch having a 100 Mbps port. The maximum transmission rate is limited only by the bandwidth of the wireless link.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

METHOD AND APPARATUS FOR A DATA TRANSMISSION OF 100 MBPS IN A TERMINAL

This is a Continuation-in-Part of Application Serial No. 08/950,028, filed October 14, 1997, the contents of which are hereby incorporated by reference. This application claims the benefit of U.S. Provisional Application Serial No. 60/086,459, entitled, "Method and Apparatus for Wireless Communication of Fast Ethernet Data Packets," filed May 22, 1998.

Field of the Invention:

The invention relates to a terminal for a wireless network for a metropolitan area wherein the terminal achieves a transmission rate of multiples of 100 Mbps for an associated wireless link. More particularly, the invention relates to a wireless terminal having a number, n, of digital processing media access control units (MACs) multiplexed to a single radio framer so as to achieve a transmission rate of n times 100 Mbps.

Background of the Invention:

Computers utilized in modern office environments are typically coupled to a local area network (LAN). The LAN allow users of the computers to share common resources, such as a common printer included in the network, and allows the users to share information files, such as by including one or more file servers in the network. In addition, the users are typically able to communicate information with each other through electronic messaging. A commonly utilized type of LAN is Ethernet. Currently, a variety of products which support Ethernet are commercially available from a variety of sources. Other types of LANs are also utilized, such as token ring, fiber distributed data interface (FDDI) or asynchronous transfer mode (ATM).

LANs are often connected to a wide area network (WAN) via a telephone modem. Thus, information is communicated over the WAN via a communication link provided by a telephone service provider. These telephone links, however, are generally designed to have a bandwidth that is sufficient for voice communication. As such, the rate at which information can be communicated over these telephone links is limited. As computers and

computer applications become more sophisticated, however, they tend to generate and process increasingly large amounts of data to be communicated. For example, the communication of computer graphics generally requires a large amount of bandwidth relative to voice communication. Thus, the telephone link can become a data communication bottleneck.

Business organizations and their affiliates are often spread over several sites in a metropolitan or geographical area. For example, a business organization can have a headquarters, one or more branch offices, and various other facilities. For such business organizations, LANs located at the various sites will generally need to communicate information with each other. Wireless communication links for connecting local area networks are known. For example, U.S. Patent No. 4,876.742, entitled "Apparatus and Method for Providing a Wireless Link Between Two Area Network Systems," and U.S. Patent No. 5,436,902, entitled "Ethernet Extender," each disclose a wireless communication link for connecting LANs.

Availability is a measure of the average number of errors which occur in digitally transmitted data. An availability of 99.99 percent is commonly required for radio communications. For an availability of 99.99 percent, the average error rate for digitally communicated data must be maintained below 1×10^{-6} errors per bit, 99.99 percent of the time. The integrity of a wireless communication link, however, is largely dependent upon transient environmental conditions, such as precipitation. Environmental precipitation causes a severe attenuation of the transmitted signal. For example, to maintain an availability of 99.99 in the presence of environmental precipitation, the signal must be transmitted at a level that is 24 dB/km higher than otherwise. Therefore, to ensure an acceptable data error rate under all expected conditions, data is typically communicated over a wireless communication link at a relatively high power and at a relatively low rate. The amount of data required to be communicated over the wireless link, however, can vary widely over time and can vary independently of environmental conditions. In addition, wireless links, especially those operated at high power levels, can cause interference with other wireless links operating in the same geographical area. Thus, the wireless link can become a data communication bottleneck.

Therefore, a technique is needed for efficiently and cost effectively communicating data over a wireless link between Ethernet local area networks.

Summary of the Invention:

The invention is a method and apparatus for achieving a data transmission rate of multiples of 100 mega-bits per second (Mbps) in a terminal for a wireless metropolitan area network. In accordance with an aspect of the present invention, a method of communicating data packets in a wireless network includes steps of receiving a first data packet wherein the first data packet is received according to a first rate of data communication, receiving a second data packet wherein the second data packet is received according to a second rate of data communication and wherein the step of receiving the second data packet is performed simultaneously with the step of receiving the first data packet, time division multiplexing the first data packet and the second data packet to a radio frame, and communicating the radio frame via a wireless link wherein the radio frame is communicated at a third rate of data communication wherein the third rate of data communication is equal to at least a sum of the first rate of data communication and the second rate of data communication. The method can also include a step of buffering the first data packet prior to time division multiplexing the first data packet such that the step of buffering the first data packet synchronizes the first data packet to the radio frame. The method can also include a step of buffering the second data packet prior to providing the second data packet to the radio framer such that the step of buffering the second data packet synchronizes the second data packet to the radio frame. The first and second data packets can be received from an Ethernet local area network. The first data packet can be a 100 mega-bit per second (Mbps) Fast Ethernet data packet. The second data packet can be a 10 Mbps Ethernet data packet. The method can include steps of receiving a third data packet, and time division multiplexing the third data packet to the radio frame. The method can include a step of encrypting the first data packet prior to performing the step of time division multiplexing.

According to another aspect of the invention, a method of communicating data packets in a wireless network includes steps of receiving a first Fast Ethernet data packet into a first MAC unit wherein the first data packet is received at a rate of 100 Mbps, receiving a second Fast Ethernet data packet into a second MAC unit wherein the second data packet is received at a rate of 100 Mbps and wherein the step of receiving the second data packet is performed simultaneously with the step of receiving the first data packet, providing the first data packet and the second data packet to a radio framer according to

time division multiplexing thereby forming a time division multiplexed radio frame, and communicating the time division multiplexed radio frame via a wireless link wherein the time division multiplexed radio frame is communicated at a rate of at least 200 Mbps. The first Fast Ethernet data packet can be received from an Ethernet local area network coupled to the first MAC unit. The method can include steps of receiving a third Fast Ethernet data packet into a third MAC unit wherein the third data packet is received at a rate of 100 Mbps, and providing the third data packet to the radio framer according to time division multiplexing. In which case, the time division multiplexed radio frame can be communicated at a rate of at least 300 Mbps. The method can include a step of buffering the first data packet in the first MAC unit prior to providing the first data packet to the radio framer. The step of buffering the first data packet can synchronize the first data packet to the radio frame. The method can also include a step of buffering the second data packet in the second MAC unit prior to providing the second data packet to the radio framer such that the step of buffering the second data packet synchronizes the second data packet to the radio frame. The method can include a step of encrypting the first data packet prior to performing the step of providing the first data packet to the radio framer. The method can also include a step of receiving an Ethernet data packet into the first MAC unit wherein the Ethernet data packet is received at a rate of 10 Mbps.

According to a further aspect of the present invention, a terminal for a wireless link in a metropolitan area includes a first data packet receiver for receiving data packets for communication over a wireless link, a second data packet receiver for receiving data packets for communication over the wireless link, a multiplexer having a first input, a second input and an output wherein the first input is coupled to receive the data packets from the first data packet receiver and wherein the second input is coupled to receive the data packets from the second data packet receiver and wherein the output of the multiplexer provides time-division multiplexed data, a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multplexed data according to radio frames, and a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link. The first data packet receiver can be a first MAC unit. In which case, the first MAC unit can include a first rate control unit, and a first rate buffer, coupled to the first rate control unit, for temporarily storing data packets received by the first MAC unit such that the data packets are provided to the first

input of the multiplexer from the first rate buffers. The first MAC unit can also include a first data encryption apparatus coupled to the first data packet switch. The first MAC unit can include a first data packet switch having a 100 Mbps port wherein the first data packet switch is coupled to the rate control unit. The first data packet switch can be a layer-two switch or a layer-three switch. The first data packet switch can include a 10 Mbps port. The 100 Mbps port can receive data packets from a local area network coupled to the terminal. The second data packet receiver can be a second MAC unit. In which case, the second MAC unit can include a second data packet switch having a 100 Mbps port. The second data packet switch can be a layer-two switch. The second MAC unit can also include a second rate control unit coupled to the second data packet switch, and a second rate buffer coupled to the second rate control unit for temporarily storing data packets received by the second data packet switch wherein the data packets are provided to the second input of the multiplexer from the second rate buffers. The first MAC unit can include a first data encryption apparatus coupled to the first data packet switch. The second MAC unit can include a second data encryption apparatus coupled to the second data packet switch.

According to yet another aspect of the present invention, a terminal for a wireless link in a metropolitan area includes a first MAC unit for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over a wireless link, n-1 additional MAC units for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over the wireless link, a multiplexer having n inputs, wherein each input is coupled to receive the data packets from a corresponding one of the first MAC unit and the n-1 additional MAC units and wherein the output of the multiplexer provides time-division multiplexed data, a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multplexed data according to radio frames, and a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link wherein the wireless link has a maximum bandwidth capacity of at least n times 100 Mbps. Each of the first MAC unit and the n-1 additional MAC units can include a rate control unit and a rate buffer coupled to the corresponding rate control unit for temporarily storing data packets received by the corresponding MAC unit prior to providing them to a corresponding one of the inputs of the multiplexer. The first MAC unit and the n-1 additional MAC units can also include an encryption apparatus coupled to

the rate buffer of the corresponding MAC unit for encrypting data packets received by the corresponding MAC unit. The first MAC unit can include a first data packet switch having a 100 Mbps port. The first data packet switch can be a layer-two switch or a layer-three switch. The first data packet switch can include a 10 Mbps port. The first MAC unit can also include a first rate control unit coupled to the first data packet switch, and a first rate buffer coupled to the first rate control unit for temporarily storing data packets received by the first data packet switch wherein the data packets are provided to the first input of the multiplexer from the first rate buffers. Each of the n-1 additional MAC units can include a corresponding data packet switch having a 100 Mbps port. Each of the first MAC unit and the n-1 additional MAC units can also include a rate control unit coupled to the corresponding data packet switch and a rate buffer coupled to the corresponding rate control unit for temporarily storing data packets prior to providing them to a corresponding one of the inputs of the multiplexer.

An advantage of the present invention is that the maximum transmission rate is limited only by the bandwidth of the wireless link.

Brief Description of the Drawings:

Fig. 1 illustrates a schematic block diagram of a pair of wireless terminals which communicate with each other via a wireless communication link in accordance with the present invention.

Figs. 2A-F illustrate representative metropolitan area network (MAN) topologies according to the present invention.

Fig. 3 illustrates a schematic block diagram of a single wireless terminal 100 in accordance with the present invention.

Fig. 4 illustrates a schematic block diagram of the digital signal processing MAC and radio framer included in the CODEC illustrated in Fig. 2.

Fig. 5 illustrates a frame structure for reformed 100BASE-T Ethernet data packets according to the present invention.

Fig. 6 illustrates a radio frame according to the present invention.

Fig. 7 illustrates a radio super frame according to the present invention.

Fig. 8 illustrates a schematic block diagram of a symbol scrambler according to the present invention.

Fig. 9 illustrates a schematic block diagram of a differential encoder and characteristic equations according to the present invention.

Fig. 10 illustrates a schematic block diagram of a differential decoder and characteristic equations according to the present invention.

Fig. 11 illustrates a mapping constellation for a constellation mapper according to the present invention.

Fig. 12 illustrates a schematic block diagram of an Ethernet-to-radio frame synchronizing portion of the rate control logic according to the present invention.

Fig. 13 illustrates a schematic block diagram of a radio frame-to-Ethernet synchronizing portion of the rate control logic according to the present invention.

Fig. 14 illustrates a schematic block diagram of a microwave module and microwave antenna according to the present invention.

Fig. 15 illustrates a perspective view of the microwave antenna and a housing for the outdoor unit according to the present invention.

Fig. 16 illustrates a schematic block diagram of an alternate embodiment of the digital signal processing MAC and radio framer according to the present invention.

Fig. 17 illustrates a frame structure for reformed 100BASE-T Ethernet data packets formed by the MAC and radio framer illustrated in Fig. 14.

Fig. 18 illustrates a schematic block diagram of an adaptive countermeasures block according to the present invention.

Fig. 19 illustrates a chart of received signal level vs. time as a result of rain fade.

Fig. 20 illustrates a flow diagram for implementing counter-measures according to the present invention.

Fig. 21 illustrates a point-to-multipoint metropolitan area network divided into sectors having inner and outer radii according to the present invention.

Fig. 22 illustrates a wireless link between two terminals wherein an unauthorized terminal is attempting to eavesdrop on communication between the two terminals.

Fig. 23 illustrates an embodiment according to the present invention having multiple digital processing MACs multiplexed to a single radio framer.

Detailed Description of a Preferred Embodiment:

Fig. 1 illustrates a schematic block diagram of a pair of wireless terminals 100, 100' which communicate with each other via a bi-directional wireless communication link 102 in accordance with the present invention. Though a single wireless communication link 102 is illustrated, it will be apparent that a network of wireless communication links can interconnect a plurality of wireless terminals, thereby forming a wireless metropolitan area network (MAN) in accordance with the present invention. Figs. 2A-F illustrate representative MAN topologies which interconnect wireless nodes A-E with wireless links according to the present invention. Each of the nodes A-E can include a wireless terminal identical to the terminal 100 or 100' illustrated in Fig. 1 for terminating each wireless link. It will be apparent that other MAN topologies can be implemented and that one or more of the nodes A-E can be coupled to one or more other types of networks.

Due to availability of portions of the radio spectrum in the 38 GHz frequency band, the wireless link 102 illustrated in Fig. 1 preferably operates within this frequency band, though another frequency band can be selected. Different channels within the selected band are assigned to nearby wireless links so as to reduce interference between them. The channels are preferably stepped at intervals of 25-50 MHz. Because the 38 GHz radio frequency band is susceptible to rain fade, the manner and path of transmissions via the wireless link 102 are adaptively modified for maintaining a predefined transmission quality in the network in accordance with the teachings of the parent application, Serial No. 08/950,028, filed October 14, 1997, the contents of which are hereby incorporated by reference.

Referring to Fig. 1, the wireless link 102 preferably includes a primary radio channel 102A which carries full duplex 100 mega-bits-per-second (Mbps) data traffic, including payload data, and an auxiliary radio channel 102B which carries full-duplex control data for network management and control over the manner of transmission over the link 102 (link control). For example, changes to the manner of transmission initiated through link control can include changing transmission power, data bit rate, amplitude modulation scheme, spectrum spreading and transmission path.

The terminal 100 includes a broadcast device, also referred to herein as an outdoor unit (ODU) 104, which terminates one end of the wireless link 102. In the preferred embodiment, the ODU 104 includes a bi-directional radio antenna and is mounted outdoors

on a roof-top mast of a building. Also included in the terminal 100 is an extender device, also referred to herein as a top floor unit (TFU) 106, which is coupled to the ODU via bi-directional communication cables 108, 110 and 112 and by power leads 114. The TFU 106 is preferably located indoors of the building having the ODU 104 located on its roof and as close as practical to the ODU 104. In preferred embodiment, the TFU 106 is located indoors, ideally in a wiring closet, on the top floor of the building. It will be apparent that the term "top floor unit", as used herein, refers to the extender unit 106 and its equivalents regardless of its location relative a building. For example, the "top floor unit" is preferably, though not necessarily, located on the top floor of a building.

The cable 108 carries full-duplex data traffic between the ODU 104 and the TFU 106 which is received from, or transmitted to, the primary radio channel 102A. The data traffic communicated via the cable 108 includes payload data for communication over the link 102 and can also include network management and control data. Preferably, data communicated via the cable 108 is in accordance with a Fast Ethernet standard, 802.3u, adopted by the Institute of Electrical and Electronics Engineers (IEEE), such as 100BASE-TX or 100BASE-T4, which operates at a data rate of 100 Mbps. The cable 110 carries half-duplex network management and control data between the ODU 104 and TFU 106. Preferably, data communicated via the cable 110 is in accordance with an Ethernet standard, such as 10BASE-T, which operates at 10 Mbps. The cable 112 carries serial data for set-up and maintenance purposes between the ODU 104 and the TFU 106. Preferably, the data communicated via the cable 112 is in accordance with conventional RS423 serial port communication protocol. The cable 114 provides supply power to the ODU 104.

Thus, in the preferred embodiment of the present invention, data is communicated between the TFU 106 and the ODU 104 via each of the cables 108, 110 and 112 according to baseband communication frequencies. This is in contrast to systems which communicate data between an indoor unit and an outdoor unit by modulating such data to intermediate frequencies (IF). The baseband communication aspect of the present invention has an advantage over such an IF modulation scheme in that implementation of the TFU 106 is simplified by the present invention. In addition, the cables 108, 110 and 112 can be of less expensive construction than would be required for IF communication.

A router or switch 116 is coupled to the TFU 106, and hence, to the terminal 100, via cables 118 and 120. The cable 118 preferably communicates data in accordance with

the 100BASE-TX or T4 Fast Ethernet standard, while the cable 120 preferably communicates data in accordance with the 10BASE-T Ethernet standard. Alternately, the cable 118 can be a fiber-optic cable, in which case, it preferably communicates data in accordance with 100BASE-FX Fast Ethernet standard.

A cable 122 is coupled to a serial port of the TFU 106. Preferably, data communicated via the cable 122 is in accordance with the RS232 serial port communication protocol. A diagnostic station 124 can be coupled to the cable 122 for performing diagnostics, set-up, and maintenance of the terminal 100. Because certain aspects of the TFU 106 and ODU 104 can only be accessed from the diagnostic station 124 security over such aspects is enhanced by the requirement that the diagnostic station 124 be directly connected to the TFU 106 via the cable 122. AC power is supplied to the TFU 106 via a power supply cable 126.

A wired local area network (LAN) 128, such as an Ethernet LAN located within the building having the terminal 100, can be coupled to the router or switch 116. In addition, a wide area network (WAN) 130, such as a telephone service network which provides access to the world wide web, can be coupled to the LAN 128. Thus, the wireless link 102 can be accessed from one or more personal computers (PCs), data terminals, workstations or other conventional digital devices included in the LAN 128 or WAN 130. A network management system (NMS) 132 is coupled to any one or more of the router or switch 116, the LAN 128 or the WAN 130. The NMS 132 accesses the wireless link 102 and the terminals 100, 100' for performing network management and link control functions (e.g. collecting data regarding operation of the MAN or changing the manner of data transmission over a particular link or links). If the NMS 132 is coupled to the LAN 128, this access is through the LAN 128. If the NMS 132 is coupled to the WAN 130, however, this access is remote via direct dial-up through a telephone service provider or via access through the world wide web. When network management and link control functions are accessed via the world wide web, a web browser is provided in the NMS 132, while a web server 236 (Fig. 3) is provided in the terminal 100. In the preferred embodiment, the DS 124 and the NMS 132 are each a personal computer, but can be another type of conventional digital device.

The terminal 100' terminates the opposite end of the link 102, remote from the terminal 100. In the preferred embodiment, the link 102 can be up to 4 kilometers or more

in dry climates (e.g. Wyoming) while maintaining 99.99% link availability and can be up to 1.2 kilometers or more in wetter climates (e.g. Florida) while maintaining 99.99% link availability. Elements illustrated in Fig. 1 having a one-to-one functional correspondence are given the same reference numeral, but are distinguished by the reference numeral being primed or not primed. Note, however, that because any NMS 132, 132' can access the wireless communication link 102 and both terminals 100, 100', an NMS 132 or 132' need not be located at each end of the link 102.

Fig. 3 illustrates a schematic block diagram of a single wireless terminal 100, including a TFU 106 and an ODU 104, in accordance with the present invention. The TFU 106 includes a 100BASE-T regenerator 200 which is coupled to the cable 118 (Fig. 1) and to the cable 108 (Fig. 1). In addition, assuming the cable 118 is a fiber-optic cable, the TFU 106 includes a converter 202 for converting between fiber-optic cable and Category 5 twisted pair cable. The converter 202 is coupled to the fiber-optic cable 118 and to the regenerator 200. The TFU 106 also includes a 10BASE-T repeater 204 coupled to the cable 120 (Fig. 1) and to the cable 110 (Fig. 1). A converter 206 included in the TFU 106 converts between signals in accordance with the RS232 standard and signals in accordance with the RS423 standard. The converter 206 is coupled to the cable 122 (Fig. 1) and to the cable 112 (Fig. 1).

The TFU 106 also includes an alternating-current to direct-current (AC/DC) power converter 208 coupled to the cable 126 (Fig. 1) and to the cable 114 (Fig. 2). The power converter 208 provides power to the TFU 106 and to the ODU 104. A status indicator 210 included in the TFU 106 displays status of the TFU 106 via light emitting diodes for diagnostic, set-up and maintenance purposes.

The TFU 106 provides three interfaces to customer equipment, including the router or switch 116 (Fig. 1) and the DS 124 (Fig. 1). These include a full-duplex 100 Mbps interface via the regenerator 200, a half-duplex 10 Mbps interface via the repeater 204 and an RS232 serial port via the converter 206. Though the payload data traffic is generally directed through the 100 Mbps interface while network management and link control traffic is generally directed through the 10 Mbps interface, a user of the terminal 100 can combine network management and link control signals with the payload data traffic in the 100 Mbps interface depending upon the particular capabilities of the router or switch 116 (Fig. 1).

The TFU 106 provides an interface from multiple indoor cables 118, 120, 122, 126, to multiple outdoor cables 108, 110, 112 and 114. TFU 106 also regenerates/repeats the Ethernet signals in the form of Ethernet data packets, between the cables 108, 118 and between the cables 110, 120. Thus, the TFU 104 serves to extend the maximum distance possible between the customer equipment, such as the router or switch 116 (Fig. 1), and the ODU 104. In the preferred embodiment, a distance between the customer equipment and the TFU 106 can be up to 100 meters while a distance between the TFU 106 and the ODU 104 can also be up to 100 meters. Accordingly, in the preferred embodiment, a distance between the customer equipment and the ODU 104 can be up to 200 meters. Because data is communicated between the TFU 106 and ODU 104 at baseband frequencies, however, apparatus for performing IF modulation is not required in the TFU 106.

The ODU 104 includes a 100BASE-T transceiver 212 coupled to the cable 108, a 10BASE-T transceiver 214 coupled to the cable 110, an RS423 driver 216 coupled to the cable 112 and a DC-to-DC power converter 218 coupled to the cable 114. The 100BASE-T transceiver 212, the 10BASE-T transceiver 214, and the RS423 driver 216 are each coupled to a coder/decoder (CODEC) 220 included in the ODU 104. The power converter 218 provides power to the ODU 104.

The CODEC 220 includes a media access control unit (MAC) 222, having a transmitting portion 224 and a receiving portion 226, a radio framer 228 and a micro-processor 230 for controlling operation of the ODU 104. The transmitting portion 224 and the receiving portion 226 of the MAC 222 are coupled to the 100BASE-T transceiver 212 for communicating Ethernet data packets with the 100BASE-T transceiver 212. The radio framer 228 is coupled to the MAC 222 for translating data from the Ethernet data packets received by the MAC 222 into a radio frames 350 (Fig. 6) suitable for radio frequency modulation and transmission. The radio framer 228 also translates received radio frames 350 (Fig. 6) into packets which it provides to the MAC 222.

The micro-processor 230 is programmed by software so as to implement a TCP/IP stack 232, a link management (LM) task 234, a HyperText Transfer Protocol (HTTP) server 236 and a simple network management protocol (SNMP) agent 238. The micro-processor 230 manages each wireless link of a network of such wireless links (e.g., a MAN), including a local link 102 (Fig. 1) which is coupled directly to the terminal 100.

The micro-processor 230 is accessible via any of the NMS 132 (Fig. 1) and via the DS 124 (Fig. 1). Thus, the wireless network of links can be managed locally, such as via an NMS 132 or DS 124 which is wired to the TFU 106. For this purpose, the microprocessor 230 is assigned an Ethernet (medium access control) MAC address. Alternately, the wireless network of links can be managed remotely, such as via an NMS 132 which is coupled to the WAN (Fig. 1) and which accesses the micro-processor 230 through internet access using TCP/IP (Internet Protocol). The TCP/IP stack 232 provides for this TCP/IP interface through the world wide web. For this purpose, the microprocessor 230 is assigned an internet protocol (IP) address.

The LM task 234 provides a function of changing the manner in which data is transmitted over a wireless link, initiated by one of the NMS 132, 132'. For example, the data rate for the link 102 can be changed via the LM task 132 included in the ODU 104. This can include sending a link control command over the link 102 to the ODU 104' (Fig. 1) so that both terminals 100, 100' communicate data at the same rate. Such commands are received from, and provided to, the microprocessor 230 by a overhead link management (OH/LM) module 240 included in the radio framer 228. Thus, the radio framer 228 appropriately combines network management and link control traffic provided by the LM task 234 with payload data received from the MAC 222 into radio frames 350 (Fig. 6) for communication over the link 102. In addition, the radio framer 228 extracts network management and link control traffic from radio frames 350 (Fig. 6) received from the link 102 and provides them to the LM task 234 of the microprocessor 230 via the OH/LM module 240. While two types of data traffic (payload and link control) are communicated via radio frames 350 (Fig. 6), the payload data is considered to be communicated via the primary channel 102A, while the link control traffic considered to be communicated via the auxiliary channel 102B. Accordingly, these two channels 102A and 102B are time-division multiplexed.

A graphical user interface by which the micro-processor 230 can be accessed from an NMS 132, 132' (Fig. 1) or DS 124, 124' (Fig. 1) for network management and link control purposes, is preferably achieved by the HTTP web server software module 236 which is implemented by the microprocessor 230 located in the ODU 104 and which is assigned a unique IP address. The server software 236 operates in conjunction with the TCP/IP stack 232. According to this aspect of the invention, the server software 236 is

utilized for providing a graphical user interface for through which network management functions are initiated. These functions include retrieving data representative of network conditions in the MAN and changing the manner in which data is transmitted across a wireless link of the MAN.

Thus, functions for managing the MAN and its wireless links can be accessed and initiated from network management stations 132, 132' (NMS) located in various portions of the MAN, utilizing web browser software resident in the NMS 132, 132'. This graphical user interface provides a user friendly environment which can operate on, and be accessed by, a variety of different NMS's obtained from a variety of different manufacturers. For example, an NMS 132, 132' can be a workstation manufactured by Sun Microsystems, a PC manufactured by any one of a variety manufacturers or even a set-top box used in conjunction with a television set. Compatibility with the web server is achieved via commercially available web browser software resident in the NMS 132, 132'. This aspect of the present invention addresses compatibility issues between the NMS 132, 132', and the terminal 100, 100'.

The SNMP agent 238 located in the ODU 104 maintains a management information database (MIB statistics) which is a collection of managed objects that correspond to resources of the MAN and of the terminal 100. The SNMP agent 238 can access the MIB to control certain aspects of the MAN and the terminal 100 and can query the MIB for information relating to the managed objects. The SNMP is accessible through the HTTP server 236.

The ODU 104 also includes a transmit modulator (TX mod) 242, a receive demodulator (RX demod) 244 and a microwave module (MWM) 246. The transmit modulator 242 translates from digital baseband output data received from the radio framer 228 to analog waveforms suitable for up-conversion to microwave frequencies and eventual transmission over the wireless link 102. The analog waveforms formed by the transmit modulator 242 preferably modulate a 490 MHz IF carrier. It will be apparent, however, that a frequency other than 490 MHz can be selected for this purpose.

The receive demodulator 244 performs functions which are essentially the opposite of those performed by the transmit modulator 242. In the preferred embodiment, the receive demodulator 244 receives a 150 MHz IF signal from the microwave module 246. It will be apparent, however, that a frequency other than 150 MHz can be selected for this

purpose. The receive demodulator 244 controls the level of the this signal via automatic gain control (AGC) and, then, down-converts the signal to baseband according to coherent carrier recovery techniques and provides this down-converted signal to the radio framer 228.

The microwave module 246 performs up-conversion to microwave frequency on the 490 MHz IF output signal generated by the transmit modulator 242 and provides this up-converted signal to a microwave antenna 508 (Fig. 12) which transmits the data over the link 102. In addition, the microwave module 246 receives a microwave frequency signal from the link 102, down-converts this signal to a 150 MHz IF signal and, then, provides this down-converted signal to the receive demodulator 244.

Fig. 4 illustrates a schematic block diagram of the digital signal processing MAC 222 and radio framer 228 included in the CODEC 220 illustrated in Fig. 2. The MAC 222 includes rate control logic 250 and rate buffers 252. The rate control logic 250 receives 100BASE-T Ethernet data packets at 100 Mbps from the 100BASE-T transceiver 212 (Fig. 3) via a media independent interface (MII) between the MAC 222 and the transceiver 212.

Note that 100BASE-T Ethernet data packets are provided to the transceiver 212 (Fig. 3) as a serial data stream. In accordance with the IEEE 802.3u standard, the serial data stream is encoded utilizing a 4B/5B scheme. According to the 4B/5B scheme, each four-bit portion (nibble) of each 100BASE-T data packet is accompanied by a 1-bit data valid field. Thus, due to the data valid bits, the wire speed for 100BASE-T is actually 125 Mbps, though the serial data communication rate is 100 Mbps assuming the data valid bits are discounted. The transceiver 212 converts this serial data stream into parallel four-bit portions of data (nibbles), a data valid signal (RX_DV) and also recovers a clock signal from the data stream. The nibbles, data valid signal and clock signal are provided to the MAC 222 by the transceiver via the MII interface.

The data nibbles, data valid signal and recovered clock signal are then synchronized to a locally generated clock signal. This locally generated clock signal preferably operates at 27.5 Mhz and is derived from a 55 MHz and 10 parts-per-million accuracy crystal oscillator located within the CODEC 220 (Fig. 3). The rate control logic 250 detects each 100BASE-T Ethernet data packet received from the transceiver 212. In the preferred embodiment, the rate control block 250 then checks each such 100BASE-T Ethernet data packet for errors utilizing the frame check sequence (FCS) appended to each 100BASE-T

Ethernet packet and strips each 100BASE-T Ethernet data packet of its preamble and start-of-frame delimiter (the frame-check sequence FCS for each 100BASE-T Ethernet packet is preferably retained). The rate control logic 250 also converts each Ethernet data packet from nibbles to bytes.

The rate control logic 250 calculates the length of each detected 100BASE-T Ethernet data packet. The rate control logic 250 also determines whether the packet is too long, too short (a runt packet) or is misaligned.

The rate control logic 250 then temporarily stores the packets in rate buffers 252. In the preferred embodiment, the bytes for each packet are clocked into the rate buffers 252 according a clock signal recovered from the data. The rate buffers 252 preferably include two first-in, first-out (FIFO) buffers having 16K entries, one for packets being transmitted and one for packets being received. The FIFO buffers each preferably provides sufficient storage for each entry so that additional information can be stored in the rate buffers 252 along with the byte of data. Such additional information preferably includes the data valid bit for each nibble and an indication of whether the nibble is payload data or overhead for the 100BASE-T Ethernet packets. For example, the overhead can include inter-packet gaps codes (e.g. one byte/octet of all zeros with associated data valid bits de-asserted), and start-of-packet codes. Assuming inter-packet gap codes are stored, preferably only one inter-packet gap code, representative of the minimum required inter-packet gap (e.g. of 0.96 μs), is stored in the rate buffers 252.

The rate control logic 250 then records the previously determined length of the 100BASE-T Ethernet data packet in a length and status FIFO buffer 254. In addition, the rate control logic 250 stores an indication of the status of the packet (e.g. too long, too short or misaligned) in the length and status buffer 254.

The radio framer 228 is coupled to the MAC 222 and includes the OH/LM block 240 (Fig. 3), a packet synch/de-synch block 254, a Reed-Solomon encoder/decoder (R-S codec) 258, a framing block 260, a pseudo-random number (PN) randomizer/de-randomizer block 262, a differential encoder/decoder 264 and a constellation mapper 266.

The packet synch/de-synch block 256 retrieves the stored 100BASE-T Ethernet data packets from the rate buffers 252 at an appropriate rate which depends, in part, upon the data transmission rate utilized for sending data over the wireless link 102. In the preferred embodiment, removal of data from the rate buffers 252 for an Ethernet packet is not

initiated until the packet has been completely stored. During periods when a complete packet is not available from the rate buffers 252, then an inter-packet gap code is substituted by the packet synch/de-synch block 254.

In the preferred embodiment of the present invention, the packet synch/de-synch block 256 reforms the 100BASE-T Ethernet data packets according to a reformed frame structure 300 for 100BASE-T Ethernet data packets illustrated in Fig. 5. The reformed frame structure 300 includes a synch pattern field 302, a length field 304, a data field 306 and a frame check sequence (FCS) field 308.

Recall that the rate control logic 250 (Fig. 4) strips each 100BASE-T Ethernet data packet of its preamble and start-of-frame delimiter prior to storing the packet in the rate buffers 252. Upon retrieving each packet from the rate buffers, the packet synch/de-synch block 256 adds a synch pattern in field 302 and a length value in field 304 to the packet. The length value is retrieved from the length and status buffer 254.

In the preferred embodiment, finite state machines control the synch/de-synch block 256 so as to enable the retrieval of 100BASE-T Ethernet packets from the rate buffers 252 along with the length and status of each, at a appropriate frequency for forming radio frames 350 (Fig. 6). A store and forward technique is applied to 100BASE-T Ethernet packets which pass through the transmit portion of the rate buffers 252. Thus, data packets to be transmitted across the wireless link 102 are completely received into the rate buffers 252 and stored therein prior to being formed into a radio frame 350. A cut-through technique, however, is preferably applied to 100BASE-T data packets which pass through the receive portion of the rate buffers 252. Thus, data packets received from the wireless link 102 are forwarded to the transceiver 212 (Fig. 3) as they received without storing the entire data packet in the rate buffers 252.

Table 1 shows the particular bit values for the synch pattern field 302 and for the length value field 304 according to the preferred embodiment of the present invention.

Table 1

Synch Field 302					Packet Length Field 304			
octet 1	octet 2	octet 3	octet 4	octet 5	octet 1	octet 2	octet 3	Bit
1	1	0	1	0	G[11]	G[7]	G[3]	7
1	1	0	1	0	G[10]	G[6]	G[2]	6
0	0	1	0	1	G[9]	G[5]	G[1]	5
1	1	0	1	0	G[8]	G[4]	G[0]	4
0	0	1	0	1	0	L[7]	L[3]	3
1	1	0	1	0	L[10]	L[6]	L[2]	2
1	1	0	1	0	L[9]	L[5]	L[1]	1
0	0	1	0	1	L[8]	L[4]	L[0]	0

As shown in Table 1, the synch pattern placed in the synch field 302 is preferably a five-octet (five-byte) pattern defined by a five-bit Willard code [11010]. Essentially, the Willard code is repeated for each octet, but is inverted for two of the five octets. The length value placed in the length field 304 is preferably an eleven-bit value L[10:0] which specifies the number of octets (bytes) of payload data contained in the data field 306. Thus, the length value L[10:0] can vary for each packet depending upon the length of the data payload included in the 100BASE-T Ethernet packet. In the preferred embodiment, a twelve-bit Golay check sum G[11:0] for the length value is stored along with the length value in the length field 304, as shown in Table 1. Because the length field 304 is preferably three octets (three bytes) a value of zero (0) is used a place holder between the length value L[10:0] and the Golay check sum G[11:0].

Referring to Fig. 5, the data payload from the Ethernet packet is stored in the data field 306. Note that 100BASE-T Ethernet data packets are conventionally of variable length. In particular, the data payload portion for a conventional 100BASE-T Ethernet packet can vary between 64 and 1518 octets (bytes). Thus, the length of the data field 304 can vary between 64 and 1518 bytes.

An important aspect of the reformation of the Ethernet data packets in the reformed frame structure 300 is the omission of the 1-bit data valid field for each nibble of the Ethernet packet. Rather, the nibbles are placed contiguously in the data field 306. This

omission of the data valid bits results in a significant savings in bandwidth required for transmitting the reformed packet frame 300 over the wireless link 102 in comparison to also transmitting the data valid bits over the wireless link 102. The FCS sequence is retained for each Ethernet packet and placed in the FCS field 308.

The packet synch/de-synch block 256 also receives link control data from the OH/LM 240 and for combining this link control data with the reformed packet frames 300 to be communicated over the link 102.

The R-S codec 258 receives the reformed data packet frames 300 and link control commands from the packet synch/de-synch block 256 and performs Reed-Solomon (R-S) forward error correction coding. The R-S encoded data is then provided to the framing block 260 where the R-S encoded data is formatted according to radio frames 350 (Fig. 6).

Fig. 6 illustrates a radio frame 350 according to the present invention. The radio frame 350 includes a synch field 352 for synchronizing a receiver to the radio frame 350, an auxiliary field 354 for network management and link control traffic which is received from the OH/LM 240 to be communicated over the auxiliary channel 102B of the wireless link 102, a data field 356, and an R-S parity field 358. The value placed in the synch field is preferably 47 hex.

In the preferred embodiment, radio frames 350 are continuously formed and transmitted across the wireless link 102 whether or not data from a complete Ethernet packet is queued in the rate buffers 252 (Fig. 4) to be placed in reformed packet frames 400. During periods when no reformed packet frames are available, the data field 356 of the current radio frame 350 is loaded with idle code (all zeros). Similarly, during periods when no network management commands are queued to be communicated via the auxiliary channel 102B, then the auxiliary field 354 is loaded with idle code (all zeros).

Recall that reformed packet frames 300 have variable length according to the preferred embodiment of the present invention. The data field 356 of each radio frame 350, however, preferably has a fixed length according to the preferred embodiment of the present invention. Accordingly, the R-S encoded data from the R-S codec 258 is placed contiguously in the data field 356 of each radio frame 350 such that reformed data frame 300 boundaries do not have a predefined relationship to radio frame 350 boundaries. For example, a reformed data frame 300 can span multiple radio frames 350. Alternately, up to three complete smaller reformed data frames 300 can be included in a single radio frame

350. Further, during idle periods between communication of reformed packets, an idle code is preferably transmitted as a place holder within the data field 356 of each radio frame 350 to meet the timing requirements needed to synchronize 100BASE-T Ethernet data packets.

As radio frames 350 are formed, multiples of the radio frames 350 are combined to form a radio "super frame" 380 (Fig. 7). Fig. 7 illustrates a radio super frame 380 according to the present invention. In the preferred embodiment, each radio super frame 380 includes 16 consecutive radio frames 350 (Fig. 6). For the first radio frame 382 of the super frame 380, the value placed in the synch field 352 is inverted (changed to B8 hex). In the second through sixteenth radio frames 384, however, the value placed in the synch field 352 remains unchanged. The value placed in the synch field 352 of the first radio frame 386 for a next radio super frame 388, is also inverted. This inversion of the synch value for the first radio frame 350 of each radio super frame 380 allows the radio super frames 500 to be detected after reception.

The radio super frame 380 is provided to the PN randomizer/de-randomizer 262. The PN randomizer/de-randomizer 262 performs quadrature amplitude modulation (QAM) scrambling on the entire radio super frame 380 except for the inverted synch values placed in the first synch field 352 of each super frame 380. By disabling the PN randomizer/ de-randomizer 262 for the inverted synch values, the scrambled super frame 380 can be detected upon reception. In preferred embodiment, the scrambling operation maps each octet (byte) of the radio super frame 380 (other than the inverted synch values) to a two successive four-bit symbols utilizing a 13th order polynomial, as shown by the schematic block diagram of the PN randomizer/de-randomizer 262 according to the preferred embodiment of the present invention.

Referring to Fig. 8, each octet of the radio super frame 380 (other than the inverted synch values) is divided into two successive four-bit portions B[3:0] which are applied to the correspondingly labelled inputs illustrated in Fig. 8. These inputs correspond to in-phase and quadrature (I&Q) symbol components I1, I0, Q1, Q0. A feedback shift register 400 generates the specified 13th order polynomial. Contents of selected memory cells of the feedback shift register 400 are exclusive-OR'd by logical exclusive-OR blocks 402, 404, 406, and 408 with each four bit portion b[3:0] of the radio frame. Outputs of the exclusive-OR blocks 402, 404, 406 and 408 form I&Q symbol components I1', I0', Q1', Q0'.

The symbol components I1', I0', Q1', Q0', are applied to the differential encoder/decoder block 264 (Fig. 4). Fig. 9 illustrates a schematic block diagram of a differential encoder 264A included in the differential encoder/decoder block 264 (Fig. 4) and characteristic equations according to the present invention. The encoder 264A forms signal components I1'', I0'', Q1'', Q0''. In the preferred embodiment, the encoder 264A is implemented by an appropriately preconditioned look-up table.

The differential encoder encodes the scrambled symbols from the PN randomizer/de-randomizer 262 such that quantum-phase differencing of the transmitted symbols according to modulo-$\pi/2$ recovers the original un-encoded data, independent of which of the four possible quantum-phase alignments is selected in the decoder 264B illustrated in Fig. 10.

Fig. 10 illustrates a schematic block diagram of the differential decoder 264B included in the differential encoder/decoder 264 (Fig. 4) and characteristic equations according to the present invention. In the preferred embodiment, the differential decoder 264B is implemented by an appropriately preconditioned look-up table.

The symbol components I1'', I0'', Q1'', Q0',' formed by the encoder 264A are applied to the constellation mapper 266 (Fig. 4). The constellation mapper 266 maps four-bit portions of the radio frame 350 to sixteen different symbols, as shown in Fig. 11, according to quadrature amplitude modulation techniques (16 QAM).

Fig. 11 illustrates a mapping constellation for the constellation mapper 266 (Fig, 4) according to the present invention. In the preferred embodiment, this constellation is defined by a standard adopted by the Digital Audio Visual Counsel (DAVIC). The input symbol components I1'', I0'', Q1'', Q0'', are mapped to the output symbol components Is, Im, Qs, Qm, as shown in Table 2. The mapped symbols are then provided by the constellation mapper 266 (Fig. 4) to the transmit modulator 242 (Fig. 3).

Table 2

I1'', I0'',Q1'',Q0'' (input)	Is, Im, Qs, Qm (output)
0000	1010
0001	1110
0010	1001
0011	1000
0100	1011
0101	1111
0110	1101
0111	1100
1000	0110
1001	0111
1010	0101
1011	0001
1100	0010
1101	0011
1110	0100
1111	0000

Received radio super frames 380 (Fig. 7) are provided to the constellation mapper 266 (Fig. 4) from the receive de-modulator 244 (Fig. 3). During radio super frame 380 reception, each radio super frame 380 is converted back from the symbols Is, Im, Qs, Qm, into the symbol components I1'', I0'', Q1'', Q0'', by the constellation mapper 262 performing a reverse of the mapping operation according to the relationships shown in Table 2.

In the preferred embodiment of the present invention, the QAM format can be altered dynamically under control of the microprocessor 230 based upon rain fade or interference detected through bit error rates (BER) or upon receiving a link control command. For example the QAM format can be dynamically altered from 16 QAM to 4 QAM. Alternately, the QAM format can be changed from 16 QAM to 4 QAM and with the application pf spectrum spreading. As a result, the data transmission bit rate falls, however, the error rate would be expected to fall also. Conversely, the QAM format can be dynamically altered from 16 QAM to 64 QAM which results in a higher data transmission bit rate.

Then, the differential decoder 264B (Fig. 10) decodes the symbol components I1'', I0'', Q1'', Q0'', into the symbol components I1', I0', Q1', Q0'. Next, the radio super frame 380 is detected by the inverted synch values for the first radio frame of each super frame 380. The symbol components I1', I0', Q1', Q0', are then provided to the PN randomizer/de-randomizer 262 (Fig. 4) which converts them to the back into the original two successive four-bit portions b[3:0] for each octet of each radio frame 350 (Fig. 6) of the radio super frame 380 (Fig. 7).

The radio frame 350 is then synchronized to the radio super frame 380 by detecting the non-inverted synch value in the field 352 (Fig. 6) for each radio frame 350. Forward error correction is performed by the R-S codec 258 (Fig. 4). For each radio frame 350 having an error which is uncorrectable by the R-S codec 258, the R-S codec 258 provides an indication, preferably by setting a flag, which is stored in the rate buffers 252 along with the affected packet data. For each Ethernet packet formed by the rate control logic 250 which is affected by such an uncorrected error as flagged by the R-S codec 258 (Fig. 4), the transmit error signal TX_ER provided to the transceiver 212 (Fig. 3) via the MII interface, is asserted. A link-layer response can then be applied to cause the packet to be resent.

The reformed data frames 300 are then passed from the R-S codec to the packet synch/de-synch block 256. In the packet synch/de-synch block 256, the reformed data frames 300 (Fig. 5), as well as network management and control data, are detected and extracted from the radio frame 350 structure. For the reformed data frames 300, this is accomplished by a windowed search technique which utilizes matched filter correlation. The search technique is utilized to locate the five-octet synch value in the synch field 302 (based on the Willard code) for each reformed data frame 300. When packet synchronization is maintained, the search window preferably encompasses only inter-packet gap periods (when the data field 356 of the radio frame 350 contains the idle code). During periods when packet synchronization is not detected, however, the search window is expanded to encompass the entire packet. Once synchronization is obtained, the window is again reduced.

Correlation searching is performed by the packet synch/de-synch block 256 utilizing a matched filter which performs correlation on an octet-by-octet basis. Accumulation by addition is performed on 40 bits of data at a time (5 bytes), as octets slide through the matched filter. The accumulated value is compared to a predetermined threshold for each octet. When the threshold is exceeded, the start of a reformed data frame 300 is indicated.

Once a synch value is detected, the length value for the packet and Golay code are read from the length field 304. The length value is verified utilizing the Golay code. If necessary, the length value is corrected utilizing the Golay code. If the length value is corrupted and uncorrectable, however, the packet is disregarded while searching for a next synch value continues.

Assuming the length value is correct or correctable, the reformed data frame 300 is loaded to the rate buffers 252 by the packet synch/de-synch block 256 in eight-bit portions (bytes) for processing into a 100BASE-T Ethernet packet. From the length value, the data valid bit for each byte is also re-generated and stored in the rate buffers 252. A single inter-packet gap code is stored in the rate buffers 252 to separate each packet. Network management and link control data from the auxiliary field 354 of each received radio frame 350 is provided to the microprocessor 230 (Fig. 3) through time-division de-multiplexing.

Then, searching for a next synch value is disabled until the end of the reformed data frame 300, as indicated by the correct or corrected length value.

Reformed data frames 300 are retrieved from the packet buffer 252 under control of the rate control logic 250 and returned to conventional 100BASE-T Ethernet format for the MII interface with the transceiver 212 (Fig. 3). This is accomplished by restoring the preamble and start-of-frame delimiter for each 100BASE-T Ethernet packet. Then, the conventional 100BASE-T Ethernet packets are provided to the 100BASE-T transceiver 212 (Fig. 3) at a rate appropriate to the 100BASE-T transceiver 212. The 100BASE-T transceiver 212 then communicates the packets to the TFU (Figs. 1 and 3). In the preferred embodiment, the rate control logic 250 includes a finite state machine for performing the function of retrieving the Ethernet packets from the rate buffers 252 and providing them to the 100BASE-T transceiver 212. Thus, the rate control logic 250 synchronizes the packets to a clock signal utilized for communication of the 100BASE-T data packets with the locally generated clock signal which is utilized for forming and communicating radio frames 350 (Fig. 6).

Referring to Figs. 3 and 4, in the preferred embodiment, the transmit modulator 242 receives four-bit symbols from the constellation mapper 266 of the radio framer 228 in the CODEC 220 at 27.5 Mbaud. Each symbol is converted to a complex in-phase and quadrature (I&Q) voltage and, then, pulse-shaped utilizing a square-root cosine filter in the transmit modulator 242. Finally, the symbol modulates a 490 MHz intermediate frequency (IF) output signal. The output level of the signal formed by the transmit modulator 242 is selectively adjustable over a continuous range under control of the micro-processor 230. Adjustments in the output level are preferably made in response to detected rain fade, detected interference or in response to a link control command. The modulated IF signal formed by the transmit modulator 242 is supplied to the microwave module 246.

The receive demodulator 244 preferably includes a 0-dB/20-dB IF attenuator in the receive path which is selectable under control of the micro-processor 230 depending upon the range of the link 102. Typically, this attenuator is set for 0-dB. For link ranges of less than approximately 50 meters, however, the attenuator is preferably set for 20-dB attenuation. The receive demodulator 244 performs adaptive slope equalization to minimize effects of distortion caused by transmission over the link 102. Further, the receive demodulator 244 preferably also includes an adaptive time-domain equalizer to perform symbol synchronization, and a matched-filter square-root-raised-cosine process is applied to minimize inter-symbol interference.

Fig. 12 illustrates a schematic block diagram of an Ethernet-to-radio frame synchronizing portion 268 of the rate control logic 250 (Fig. 4) and transmit buffer 252A according to the present invention. The transmit buffer 252A forms a portion of the rate buffers 252 (Fig. 4). 100BASE-T Fast Ethernet packets and a receive data valid signal RXDV are received into the transmit buffer 252A from the transceiver 212, as explained above in reference to Fig. 4. In addition, a clock signal at 25 MHz is derived from the incoming data packet and utilized for clocking the incoming Ethernet data packets into the transmit buffer 252A.

The receive data valid signal RXDV is provided to a first input of an arbitration logic block 270. In response to a complete Ethernet packet being stored in the transmit buffer 252A, as indicated by the data valid signal RXDV, the arbitration logic 270 instructs a packet counter 272 to increment a count by one. As Ethernet packets are retrieved from the transmit buffer 252A, a delayed data valid signal is also retrieved from the transmit buffer 252A. This delayed data valid signal is applied to a second input to the arbitration logic block 270. In response to a complete Ethernet data packet being removed from the transmit buffers 252A as it is supplied to the synch/de-synch logic block 256, as indicated by the delayed data valid signal, the arbitration logic block 282 instructs the packet counter 272 to decrement the count by one. Thus, the packet counter 272 maintains a current count of complete Ethernet data packets in the transmit buffer 252A.

This count is provided by the packet counter 272 to a threshold compare block 274. The threshold compare block 274 notifies a read packet state machine 276 when a sufficient number of complete Ethernet packets are stored in the transmit buffer 252A to initiate retrieval of the packets from the transmit buffer 252A. In the preferred embodiment, only one complete Ethernet packet need be stored in the transmit buffer 252A to initiate the read packet state machine 276 to retrieve the packet. Once initiated to retrieve a packet, the read state machine 276 activates a first input to a logic AND gate 278. A second input to the logic AND gate 278 receives a read frame enable signal from the synch/de-synch logic 256 (Fig. 4). This read frame enable signal is activated when the synch/de-synch logic 256 is ready to receive the Ethernet packet data for insertion into a radio frame 350 (Fig. 6).

An output of the logic AND gate 278 is coupled to a read input of the transmit buffer 252A for retrieving the packet from the transmit buffer 252A. As it is being

retrieved, the packet is provided to the synch/de-synch logic 256.

An important aspect of the Ethernet-to-radio frame synchronizing portion 268 of the rate control logic 250 (Fig. 4) is that it synchronizes the receiving of Ethernet data packets according to 25 MHz clock signal which is asynchronous with the locally generated clock signal. Note that the 25 MHz clock signal is derived from the incoming Ethernet data packets and is applied to the transmit buffer 252A for storing the packet data while the locally generated clock signal is applied to the transmit buffer 252A for retrieving Ethernet packet data from the transmit buffer. Thus, the arbitration logic, packet counter 272 and threshold compare logic 274 operate according to the derived 25 MHz clock, while the read packet state machine 276 and the radio framer 228 (Fig. 4) operate according to the locally generated clock.

In the preferred embodiment, the locally generated clock signal is 27.5 MHz. Because the locally generated clock signal is at a higher rate than the clock signal derived from the incoming Ethernet packets, in absence of the synchronizing portion 268 of the rate control logic 250, it would be possible for the transmit buffer 252A to become empty while an Ethernet packet is still being received into the transmit buffer 252A. Thus, the synchronizing portion 268 of the rate control logic 250 avoids this potential problem.

Assuming that an adaptive counter measure is employed which reduces the rate at which radio frames 350 (Fig. 6) are formed, this also reduces the rate at which the data from Ethernet packets is retrieved from the transmit buffer 252A. Assuming this rate is below 25 MHz (e.g. 13.75 MHz), then a complete packet need not be stored in the transmit buffer 252A prior to initiating retrieval of such a packet. In the preferred embodiment, under such circumstances, cut-through is employed wherein the incoming Ethernet data packet is supplied to the radio framer 228 (Fig. 4) prior to the complete packet being received into the transmit buffer 252A.

Fig. 13 illustrates a schematic block diagram of a radio frame-to-Ethernet synchronizing portion 280 of the rate control logic 250 (Fig. 4) according to the present invention. The receive buffer 252B forms a portion of the rate buffers 252 (Fig. 4). 100BASE-T Fast Ethernet packets recovered from radio frames 350 (Fig. 6), and a recovered receive data valid signal RXDV, are received into the receive buffer 252B from the synch/de-synch block 256, as explained above in reference to Fig. 4. The internally generated clock signal at 27.5 MHz is synchronous with the radio frames 350 (Fig. 6) and

utilized for clocking the incoming Ethernet data packets into the receive buffer 252B. Ethernet data packets stored in the receive buffer 252B are retrieved and provided to the transceiver 212 (Fig. 3) according to a 25 MHz clock.

If no spectrum spreading is employed for data communicated via the link 102, then the clock signal utilized for clocking data into the receive buffer 252B preferably operates at 27.5 MHz. Because the clock signal utilized for retrieving data from the receive buffer 252B preferably operates at 25 MHz, there is no possibility that the receive buffer 252B will become empty while an Ethernet packet is still being received into the receive buffer 252B.

However, in the event that spectrum spreading is employed for data communicated via the link 102, however, the clock signal applied to the receive buffer 252B can operate at a lower frequency (e.g. 13.75 MHz), that is synchronous with the internally generated 27.5 MHz clock signal. In which case, it would be possible for the receive buffer 252B to become empty while an Ethernet packet is still being received into the receive buffer 252B. Thus, the synchronizing portion 280 of the rate control logic 250 avoids this potential problem, as explained below.

The recovered receive data valid signal is provided by the synch/de-synch block 256 (Fig. 4) to a first input of an arbitration logic block 282 and to a read packet state machine 288. In response to a complete Ethernet packet being stored in the receive buffer 252B, as indicated by the recovered data valid signal, the arbitration logic 282 instructs a packet counter 284 to increment a count by one. As Ethernet packets are retrieved from the receive buffer 252B, a data valid signal RXDV is also retrieved from the receive buffer 252B. This data valid signal RXDV is utilized by the transceiver 212 (Fig. 3) and applied to a second input to the arbitration logic block 282. In response to a complete Ethernet data packet being removed from the receive buffer 252B, and supplied to the transceiver 212 (Fig. 3), as indicated by the data valid signal RXDV, the arbitration logic block 282 instructs the packet counter 284 to decrement the count by one. Thus, the packet counter 284 maintains a current count of complete Ethernet data packets in the receive buffer 252B.

This count is provided by the packet counter 284 to a threshold compare block 286. The threshold compare block 286 notifies a read packet state machine 288 when a sufficient number of complete Ethernet packets are stored in the receive buffer 252B to

initiate retrieval of the packets from the receive buffer 252B. In the preferred embodiment, only one complete Ethernet packet need be stored in the receive buffer 252B to initiate the read packet state machine 288 to retrieve the packet. Once initiated to retrieve a packet, the read state machine 288 activates a first input to a logic AND gate 290. A second input to the logic AND gate 290 receives a LAN read clock enable signal from the transceiver 212 (Fig. 3). This LAN read clock enable signal is activated when the transceiver 212 is ready to receive the Ethernet packet data for communication to the TFU 106 (Fig. 1).

An output of the logic AND gate 290 is coupled to a read input of the receive buffer 252B for retrieving the packet from the receive buffer 252B. As it is being retrieved, the packet is provided to the transceiver 212. Accordingly, this aspect of the present invention prevents the receive buffer 252B from being emptied while a packet is being provided from the receive buffer 252B to the transceiver 212 (Fig. 3).

A first alternate approach for avoiding overflow in the receive buffer 252B of the terminal 100 during periods when data is being communicated over the wireless link 102 according to maximum transmission rates can be implemented when an Ethernet data source (e.g. a terminal in the LAN 128') is operating at a slightly higher rate than the reference clock utilized for removing data from the receive buffer 252B. This approach includes monitoring the current depth of the receive buffer 252B, and as the amount of occupied storage space increases, then the transmission rate of the Ethernet data source is adjusted upward utilizing a voltage controlled oscillator. As the amount of occupied storage space decreases, then the transmission rate of the transceiver 212 is adjusted downward. When the buffer is nearly empty, the transmission rate is set to the nominal level of 25 Mhz. Both the originating and local frequency references must be within 100 parts per million high or low of the IEEE 802.3 Ethernet specified 25 MHz.

A second alternate approach for avoiding overflow in the receive buffer 252B of the terminal 100 during periods when data is being communicated over the wireless link 102 according to maximum transmission rates, involves reducing the minimum inter-packet gap utilized for forwarding packets removed from the receive buffer 252B. For example, rather than utilizing 12 byte-times to represent the inter-packet gap, the inter-packet can be represented by 11 byte-times. This may result in a violation of the IEEE 802.3 standard for the minimum inter-packet gap, however, this result is expected to be more desirable than the loss of packet data should the receive buffer 252B overflow.

A third alternate approach for avoiding overflow in the receive buffer 252B of the terminal 100 during periods when data is being communicated over the wireless link 102 according to maximum transmission rates, is for the microprocessor 230 of the terminal 100 to send a link control command to the terminal 100'. This link control command provides a pause packet to the layer-two switch 600' (the layer-two switch 600' and associated packet buffers 602' are not shown, however, because the terminal 100' is identical to the terminal 100, it will be understood that the layer-two switch 600 and packet buffers 602 illustrated in Fig. 16 have identical counter-parts in the terminal 100', referred to herein as 600' and 602'). The pause packet causes the switch 600' to temporarily store packets in its associated packet buffers 602' rather than sending such packets to the receive buffer 252B.

Fig. 14 illustrates a schematic block diagram of the microwave module (MWM) 246 (Fig. 3) and microwave antenna 508 according to the present invention. The MWM module 246 constitutes a wireless transceiver for implementing wireless communication over the link 102 (Fig. 1). The MWM 246 includes a transmit up-converter (TX-U/C) 500 coupled to receive signals from the transmit modulator 242. The TX U/C 500 up-converts 490 MHz IF signals received from the transmit modulator 242 to microwave frequency for transmission over the link 102. In the preferred embodiment, the frequency of transmission over the link 102 is selectable under control of the micro-processor 230 in 12.5 MHz steps across two adjacent microwave bands (e.g. 38.6-39.2 GHz and 39.3-40.0 GHz).

A transmit power amplifier (TX-P/A) 502 coupled to the transmit up-converter 500 amplifies the microwave signals provided by the transmit up-converter 500 to an appropriate level. In the preferred embodiment, the transmit power amplifier 502 has a 1-dB compression point at about 17 dBm. The nominal power is preferably set to 11 dBm, however, the transmit power is selectively controllable by the micro-processor 230 in response to detected rain fade, detected interference or in response to a link control command.

A transmit sub-band filter 504 coupled to the output of the transmit power amplifier 502 filters unwanted frequencies from the microwave signal to be transmitted over the link 102. The microwave module 246 includes a di-plexer 506 coupled to the transmit sub-band filter 504. The di-plexer 506 couples the microwave module 246 to the microwave antenna 508 for full-duplex communication over the link 102 by the microwave module

246. The antenna 508 transmits microwave signals over the link 102 and receives microwave signals from the link 102.

A microwave signal received from the link 102 by the antenna 508 is provided to a receive sub-band filter 510 via the di-plexer 506. The receive sub-band filter 510 filters unwanted frequencies from the received signal and provides a filtered signal to a low noise amplifier (LNA) 512. Then, the received signal is down-converted, preferably to 150 MHz IF by a receive down-converter (RX D/C) 514. It will be apparent, however, that a frequency other than 150 MHz can be selected. An intermediate frequency automatic gain control (IF AGC) circuit 516 adjusts the level of the down-converted signal to a predetermined level. An output formed by the IF AGC 516 circuit 514 is provided to the receive demodulator 244.

According to the preferred embodiment of the present invention, a microwave frequency synthesizer 518 included in the microwave module 246 is locked to a precision crystal reference signal and is digitally controlled by the microprocessor 230 (Fig. 3) with a 12.5 Mhz step capability. Two outputs of the frequency synthesizer 516 are each locked to the same crystal reference signal and provided to the transmit up-converter 500 and to the receive down-converter 514 for performing up-conversion and down-conversion, respectively.

Fig. 15 illustrates a perspective view of the microwave antenna 508 and a housing 550 for the outdoor unit 104 (Figs. 1 and 3) according to the present invention. The housing 550 protects the ODU 104 from environmental conditions, such a rain, snow and sunlight, which can be encountered on roof-tops where the ODU 104 is typically positioned. The housing 550 includes a flange 552 for attaching the antenna 508 and cooling fins 554 for dissipating heat generated by the electrical circuits of the ODU 104. A cable 556 which is preferably weather-resistant and electrically-shielded, extends between, and electrically connects, the ODU 104 to the TFU 106 (Figs. 1 and 3). Thus, the cable 556 includes each of the cables 108, 110, 112 and 114 (Figs. 1 and 3).

Fig. 16 illustrates a schematic block diagram of an alternate embodiment of the digital signal processing MAC 222' and radio framer 228' according to the present invention. Elements illustrated in Fig. 16 having a one-to-one functional correspondence with elements illustrated in Fig. 4 are given the same reference numeral, but are distinguished by the reference numeral being primed. In one respect, the arrangement

illustrated in Fig. 16 differs from that illustrated in Fig. 4 in that a layer-two switch 600 and associated packet buffer 602 are added.

According to the embodiment of the MAC 222' illustrated in Fig. 16, the Ethernet switch 600 is coupled to the transceivers 212, 214 (Fig. 3) and to packet buffers 602. The packet buffers 602 provide a temporary storage for packets while being directed through the switch 600. The switch 600 is also coupled to the microprocessor 230 via an interface 604 and to the rate control logic 250' via an interface 606. The switch 600 can be a conventional layer-two Ethernet network switch having a 100BASE-T port coupled to the cable 108 and a 10BASE-T port coupled to the cable 110. In the preferred embodiment, the switch 600 also includes a 10BASE-T port which is coupled to the microprocessor 230 via the interface 604 and a 100BASE-T MII port which is coupled to the rate control logic 250' via the interface 606.

Network management and link control traffic in the form of Ethernet packets received by the switch 600 from the transceiver 212, the transceiver 214, or the interface 606, and which include the MAC address of the microprocessor 230 as a destination address are directed to the microprocessor 230 via the interface 604 by the switch 600. Similarly, the microprocessor 230 sends Ethernet packets to the rate control logic 250' via the switch 600 for communication over the link 102 and to the transceivers 212, 214 via the switch 600 for communication with the router or switch 116 (Fig. 1).

In the preferred embodiment, the switch 600 implements a flow control technique in accordance with IEEE 802.3x. According to the present invention, the flow control technique is selectively initiated by the rate control logic 250' sending a pause packet to the switch 600 via the interface 606. Each pause packet includes an indication of a how long the flow control technique is to remain active. In response to receiving the pause packet, the switch 600 does not provide packets which are received from the transceivers 212, 214 or from the interface 604 to the interface 606. Rather, when the flow control technique is active, the switch 600 temporarily queues such packets by storing them in the packet buffers 602. The pause signal can preferably be initiated for several hundred milli-seconds while packets are received from the transceivers 212, 214 or from the interface 604 without loss of any such packets. When the indicated time expires, the flow control technique is deactivated. Upon deactivation of the flow control technique, the switch 600 retrieves the queued packets from the packet buffers 602 and provides them to the rate

control logic 250' via the interface 606.

The rate control logic 250' sends a pause packet with an indicated activation period in response to a halt control signal received from the rate buffers 252' via a signal line 608. When activated, the halt signal provided via the signal line 608 indicates that the rate buffers 252' are nearly full. The indicated activation period included in the pause packet is appropriate to allow sufficient data to be removed from the rate buffers 252' and communicated over the link 102 via radio frames 350.

As an example of operation of the MAC 222', assume that rain fade or interference is detected in the link 102 by an increase in a measured bit error rate (BER). In response, a link control command is issued by the microprocessor 230 which causes the data rate for the link 102 to be reduced. As a result of this lower data rate for the link 102, radio frames 350 are formed less quickly and, thus, data is removed from the rate buffers 252' at a lower rate. If the reduced data rate results in the rate buffers 252' becoming nearly full, the rate buffers 252' activate the halt signal via the signal line 608. In response, the rate control logic 250' sends a pause packet to the switch 600. Then, while flow control is active, packets received from the transceiver 212, 214 or the interface 604 for communication over the link 102 are temporarily queued in the packet buffers 602. Accordingly, the MAC 222' according to the present invention implements a flow control technique for adapting a current rate of data transmission over the link 102 to a rate at which Ethernet packets are received by the MAC 222' from the TFU 106 (Figs. 1 and 3), without loss of the Ethernet packets.

In addition, the embodiment of the MAC 222' illustrated in Fig. 16 includes an encryption/decryption block 612 coupled between the rate control logic 250' and the rate buffers 252'. Accordingly, for packets to be transmitted over the link 102, the encryption/decryption block 612 encrypts the Ethernet data packets prior to temporarily storing the data packet in the rate buffers 252'. Conversely, Ethernet packets received from the link 102 are decrypted by the encryption/decryption block 612 before being provided to the switch 600. A memory buffer 614 coupled to the encryption/decryption block 612 provides a temporary memory store for use during encryption/decryption of the Ethernet packets. An encryption start control signal line 610 coupled between the encryption/decryption block 612 and the length/status buffer 254' is utilized by the encryption/decryption block 612 to instruct the length/status buffer 254' to provide an

encryption tag and sequence number to the packet synch/de-synch block 256'. This arrangement which includes the encryption/decryption block 612 provides an advantage over the arrangement illustrated in Fig. 4 in that data security is enhanced.

Fig. 17 illustrates a frame structure 700 for reformed 100BASE-T Ethernet data packets formed by the MAC 222' and radio framer 228' illustrated in Fig. 16. When the packet is removed from the rate buffers 252' and reformed for insertion to a radio frame 350 (Fig. 6), the encryption tag and sequence number provided by the length/status buffer 254' (Fig. 16) are appended to the reformed packet frame 700 in an encryption tag field 702 and a sequence number field 704, respectively. The encryption tag indicates an appropriate key box utilized to encrypt the data while the sequence number provides synchronization information to the terminal which receives the reformed Ethernet data frame 700 from the wireless link 102. Fields of the reformed packet frame 700 illustrated in Fig. 17 which have one-to-one functional correspondence with those illustrated in Fig. 5 are given the same reference numeral primed.

Referring to Fig. 16, this arrangement also differs from that illustrated in Fig. 4 in that the PN randomizer/de-randomizer 262 and the differential encoder/decoder 264 are omitted and, instead, an adaptive countermeasures block 616 takes their place. The adaptive countermeasures block 616 responds to a rate change command issued by the microprocessor 230 by changing the rate at which data is communicated over the wireless link 102. The rate at which data is communicated can be in response to a detected increase in BER due to rain fade or can be to reduce interference with nearby wireless links, such as to reduce interference between subscriber terminals in a point-to-multipoint network.

Fig. 18 illustrates a schematic block diagram of the adaptive countermeasures block 616 according to the present invention. A multiplexer 750 is coupled to the framing block 260' (Fig. 16) for communicating radio super frames 380 (Fig. 7) with the framing block 260'. A first PN randomizer/de-randomizer 262A', a second PN randomizer/de-randomizer 262B' and a first differential encoder/de-coder 264A' are each coupled to receive selected radio super frames 380 from the multiplexer 750 depending upon conditioning of the multiplexer 750 by the rate change control signal.

In the preferred embodiment, the PN randomizer/de-randomizers 262A', 262B, 262C' perform scrambling on the radio super frames 380 in an identical manner to the PN randomizer /de-randomizer 262 illustrated in Figs. 4 and 8. Super frames 380 scrambled

by the PN randomizer/de-randomizer 262A' are provided to a second differential encoder/decoder 264B'. The differential encoder /decoders 264A', 264B' and 264C' preferably perform encoding and decoding in an identical manner to the differential encoder/de-coder 264 illustrated in Fig. 4. Then, super frames 380 encoded by the second encoder/decoder 264B' are provided to a QAM constellation mapper 266'. The QAM constellation mapper 266' preferably performs QAM constellation mapping in an identical manner to the QAM constellation mapper 266 illustrated in Figs. 4 and 16. A multiplexer 756 is coupled to the QAM constellation mapper 266' for communicating encoded radio super frames 380 with the Rx demodulator 244 (Fig. 3) and Tx modulator 242 (Fig. 3). Thus, when a first path through the PN randomizer/de-randomizer 262A', the second differential encoder/decoder 264B' and QAM constellation mapper 266' is selected, radio super frames 380 are conditioned identically for transmission and reception as when passing through the PN randomizer/de-randomizer 262, differential encoder/decoder 264 and QAM constellation mapper illustrated in Fig. 4. In the preferred embodiment, the first path conditions the radio super frames 380 according to 16 QAM.

The third differential encoder/decoder 264C' is coupled to the PN randomizer/de-randomizer 262B' and to a quadrature phase-shift (QPSK) constellation mapper 752A. The QPSK constellation mapper 752A maps portions of the radio frame 350 to QPSK symbols according to quadrature phase-shift keying techniques (QPSK). Super frames 380 are communicated between the QPSK constellation mapper 752A and the multiplexer 756. Thus, when a second path through the PN randomizer/de-randomizer 262B', the differential encoder/decoder 264C' and QPSK constellation mapper 752A is selected, radio super frames 380 are conditioned for transmission and reception according to QPSK format.

A second QPSK constellation mapper 752B is coupled to the differential encoder/decoder 264A' and to a PN randomizer/de-randomizer 262C'. The QPSK constellation mapper 752B maps portions of the radio frame 350 to QPSK symbols according to quadrature phase-shift keying techniques (QPSK) identically to the QPSK constellation mapper 752A. Super frames 380 are communicated between the QPSK constellation mapper 752B and the multi-plexer 756. Thus, when a third path through the differential encoder/decoder 264A', QPSK constellation mapper 752B and PN randomizer/de-randomizer 262C', is selected, radio super frames 380 are conditioned for transmission and reception according to QPSK format with spectrum spreading. Upon

reception, super frames 380 routed through this third path are appropriately de-spreaded and decoded for communication with the framing block 260'.

So that the radio super frames 380 are properly received by a receiving terminal (e.g. the terminal 100 illustrated in Fig. 1), it is important the appropriate path is selected through the adaptive countermeasures block 616 for each radio super frame 380. This can be accomplished by the transmitting terminal 100 notifying the receiving terminal 100' of the manner and rate at which the transmitting terminal 100 is transmitting radio super frames 380.

Fig. 19 illustrates a chart of received signal level vs. time as a result of rain fade. Refer to Figs. 1 and 20 and assume that the terminal 100 is receiving data from the terminal 100' via the wireless link 102. When rain occurs between the terminals 100 and 100', the level of the microwave carrier signal received by the terminal 100, the received signal level (RSL) falls over time as the rain increases over time. Thus, depending upon the weather conditions, the RSL can eventually fall from a normal level to below threshold levels set at L1-L8. When the RSL is above the threshold level L1, this represents an insubstantial level of rain fade. However, when the RSL is below the threshold level L8, this represents a extreme level of rain fade. The threshold levels L2-L7 represent progressively increasing levels of rain fade between the extremes represented by L1 and L8. The rate at which the RSL falls (the measured slope) can also vary depending upon the weather conditions. Similarly, as the weather conditions improve, the RSL can return the normal level. In response to rain fade, the bit error rate (BER) tends to rise. Thus, the adaptive countermeasures implemented by the present invention can detect the presence of rain fade by measuring the RSL or the BER.

In addition, the BER tends to rise in response to interference between nearby wireless links. A significant difference between rain fade and interference, however, is that in the event of interference, the RSL can remain at a normal level while the BER rises. Accordingly, the adaptive countermeasures implemented by the present invention can detect the effects of interference by measuring the BER.

Accordingly, in the preferred embodiment, the present invention responds to both the measured RSL and the measured BER. To simplify the following discussion, an example involves a response to rain fade detected by measuring the RSL. It will be apparent, however, that an identical response can be made by measuring the BER. Thus,

in the following discussion, the BER, rather than the RSL, is compared to the various thresholds disclosed (in addition, the operators > and < are exchanged with each other). In addition, it will be apparent that a response can be made simultaneously to both the RSL and to the BER with appropriate modifications.

Fig. 20 illustrates a flow diagram for implementing counter-measures according to the present invention in response to measured RSL. In the preferred embodiment, the microprocessor 230 (Fig. 3) is appropriately programmed to implement the flow diagram illustrated in Fig. 20. In a first state 800, the terminal 100 is configured for communicating data at 16 QAM. Then, program flow moves from the state 800 to a state 802. In the state 802 a determination is made whether the RSL has fallen below the threshold level L1. If the RSL has not fallen below the threshold level L1, then program flow returns to the state 800.

If, however, the RSL has fallen below the threshold level L2, then program flow moves to a state 804. In the state 804, a determination is made whether the rate at which the RSL is changing exceeds a first predefined slope Z1. If the rate does not exceed the predefined slope Z1, then program flow moves from the state 804 to a state 806. In the state 806, a determination is made whether the RSL has fallen below the threshold L4. If the RSL has not fallen below the threshold L4, then program flow returns to the state 800.

If, however, the RSL has fallen below the threshold L4, then program flow moves from the state 806 to a state 808. If the determination made in the state 804 resulted in a determination that the rate did exceed the predefined slope Z1, then the program flow moves from the state 804 to a state 808. In the state 808, the terminal is configured to transmit data according to QPSK (without spectrum spreading). Then program flow moves from the state 808 to a state 810.

In the state 810, a determination is made as to whether the RSL is above the threshold L5. If the RSL is above the level L5, then program flow moves from the state 810 to a state 812. In the state 812, a determination is made as to whether the rate at which the RSL is changing exceeds a predefined slope Z2. If the rate exceeds the slope Z2, then program flow returns to the state 800. If the rate does not exceed the slope Z2, then program flow moves from the state 812 to a state 814.

In the state 814, a determination is made whether the RSL is above the threshold level L1. If not, then program flow returns to the state 808. If in the state 814, the RSL is above the threshold L1, then program flow returns to the state 800.

If, in the state 810, the RSL is not above the threshold L5, then program flow moves to a state 816. In the state 816, a determination is made whether the RSL is below the threshold L6. If the RSL is not below the threshold L6, program flow returns to the state 808. If, in the state 816, the RSL is below the threshold 816, then program flow moves from the state 816 to a state 818. In the state 816, a determination is made if the rate of change in the RSL exceeds a predefined slope Z3. If the slope Z3 is not exceeded program flow moves from the state 818 to a state 820.

In the state 820, a determination is made whether the RSL is below the threshold L8. If not, then program flow returns to the state 808. If in the state 820 the RSL is not below the threshold L8, the program flow moves to a state 822. In addition, if, in the state 818, the slope Z3 is exceeded, program flow moves to the state 822. In the state 822 the terminal 100 is configured for communicating data according to QPSK with spectrum spreading.

From the state 822, program flow moves to a state 824. In the state 824, a determination is made whether the RSL is below the threshold L7. If the RSL is not below the level L7, then program flow returns to the state 822. If, in the state 824, the RSL is above the threshold L7, then program flow moves from the state 824 to a state 826. In the state 826, a determination is made whether the rate of change in the RSL exceeds a predefined slope Z4. If so, program flow returns to the state 808. If. in the state 826, the slope Z4 is not exceeded, then program flow moves to a state 828.

In the state 828, a determination is made whether the RSL is above the threshold 828. If so, program flow returns to the state 808. If, in the state 828, the RSL is not above the threshold 828, then program flow returns to the state 822.

An important aspect of the present invention is that hysteresis is introduced in the flow diagram for changing the manner of data communication in the states 800, 808 and 822, based upon the RSL. Thus, for example, to change from 16 QAM to QPSK, the RSL must fall below L2. However, to change from QPSK to 16 QAM, the RSL must rise above L1 where L1 is higher than L2. This hysteresis reduces the frequency at which the manner of communicating data is changed and prevents oscillations from occurring between any two of the states 800, 808 and 822.

In a point-to-multipoint MAN, a single network node communicates radio super frames 380 with a plurality of other nodes. Fig. 21 illustrates a point-to-multipoint metropolitan area network divided into sectors having inner and outer radii according to the present invention. A single node at a hub 900 communicates with a plurality of subscriber nodes, designated "r" located as various radial distances from the hub 900 and in different directions (sectors). An important advantage of the present invention that changes in manner in which data is communicated over a wireless link can be utilized to reduce interference between nodes in a same sector, but at a different radial distances from the hub 900.

As an example, assume a first subscriber node 902 is located in a sector 904 at a radial distance from the hub 900 that is less than 2 Km. Assume that a second subscriber node 906 is also located in the in the sector 904 but at a radial distance from the hub 900 that is more than 2 Km and less than 4 Km. If both subscriber nodes 902, 906 communicate with the hub 900 in the same manner, there is a probability that communications intended for the node 902 will interfere with communications intended for the node 906. In the preferred embodiment of the present invention, however, the adaptive countermeasures block 616 (Figs. 14 and 16) of the first subscriber node 902 is conditioned to communicate data in a first manner (e.g. according to 16 QAM), whereas, the adaptive countermeasures block 616 of the second subscriber node 906 is conditioned to communicate data in a second manner (e.g. according to QPSK). The adaptive countermeasures block 616 of hub 900 is conditioned for communication with either of the nodes 902, 906, by changing back and forth between the first and second manner of communicating. This is accomplished by appropriately conditioning the rate control signal applied to the multiplexers 750, 756 (Fig. 18) of the hub 900 depending upon which node 902, 906 the hub is currently communicating with.

In the preferred embodiment of the present invention, a security authentication protocol is implemented for data security purposes against eavesdroppers. Fig. 22 illustrates a wireless link 102 between two terminals 100 and 100' wherein an unauthorized terminal 950 is attempting to eavesdrop on communication between the two terminals 100, 100'. Each terminal 100, 100' and 950 is preconditioned to periodically authenticate the other terminal opposite the communication link. For this purpose, each terminal is assigned a unique password.

Link authentication is accomplished in the following manner: Once communication between the terminals 100 and 100' is established, the terminals 100, 100' exchange their passwords. Then, at periodic intervals, the terminal 100 sends a challenge message to the terminal 100'. The challenge message includes an identification number and a random number. The terminal 100' receives the random number and calculates a response based upon a mathematical combination of the random number and its unique password. Then the terminal 100' then sends the calculated response to the terminal 100 along with the same identification number it received.

The terminal 100 then matches the identification number it receives from the terminal 100' to the challenge message it previously sent and then compares the response it received to an expected response. The terminal 100' determines the expected response based upon its knowledge of the unique password associated with the terminal 100' and upon its knowledge of the random number included in the challenge. If the received response matches the expected response, the terminal 100' sends a success message to the terminal 100'. Data communication then resumes. Each terminal 100, 100' periodically authenticates the other in a symmetrical manner.

If, however, the received response does not match the expected response, an alarm is set in the terminal 100. In response to the alarm, the terminal 100 maintains the wireless communication link 102 by sending and receiving radio frames 350 (Fig. 6) with the terminal 100, however, the radio frames 350 sent by the terminal 100 no longer carry 100BASE-T Ethernet data. Instead, the inter-packet gap code is sent. In addition, the terminal 100 is configured to no longer detect and separate 100BASE-T Ethernet packets from received radio frames. Thus, the 100BASE-T traffic in both directions is disabled. The terminals continue attempting to re-authenticate the link, and if successful, communication of 100BASE-T packets resumes.

It is important to note that each terminal 100, 100', 950, is configured to successfully receive radio frames at all times, but us configured to successfully receive 100BASE-T packet data only if it receives a response to a challenge message which matches an expected response. The determination of whether a response to a challenge message is appropriate depends upon knowledge of the random number included in the challenge message.

Assume that once the link 102 is established, the terminal 950 attempts to eavesdrop. This is an unauthorized intruder who is attempting to receive data from the link. It is expected in such a situation, that the terminal 950 will have its transmitter muted in an attempt to escape detection. Because the transmitter of the terminal 950 is muted, it cannot authenticate with either terminal 100, 100'. Thus, although the terminal can receive responses to challenge messages sent by the terminals 100, 100', it cannot match such a response to an expected response because the terminal 950 will not have knowledge of the random number sent with the response. Thus, an alarm will be set in the terminal 950. Once this occurs, the terminal 950 can no longer receive 100BASE-T packet data. Accordingly, the attempted eavesdropping is prevented and data security maintained.

Fig. 23 illustrates an embodiment according to the present invention having multiple digital processing MACs 222A'', 222B'' multiplexed to a single radio framer 228''. The MACs 222A'', 222B'' can each be identical to the MAC 222' illustrated in Fig. 16 while the radio framer 228'' can be identical to the radio framer 228' illustrated in Fig. 16. This embodiment enables multiple 100BASE-T Ethernet packets to be received simultaneously, one for each MAC 222A'', 222B''. The Ethernet packets are temporarily stored in each MAC 222A'', 222'' and then provided to the radio framer 228'' via a multiplexer 980 according to time division multiplexing. The time division multiplexed data is then communicated over the wireless link 102. According to this embodiment, the wireless link 102 is configured to communicate data at 200 Mbps. It will be apparent that a number, n, of MACs can be coupled to the multiplexer 980 thereby achieving a n x 100Mbps data rate for the wireless link 102. Such an arrangement is limited by the maximum bandwidth capacity for the wireless link 102.

The present invention has been described in terms of specific embodiments incorporating details to facilitate the understanding of the principles of construction and

operation of the invention. Such reference herein to specific embodiments and details thereof is not intended to limit the scope of the claims appended hereto. It will be apparent to those skilled in the art that modifications may be made in the embodiment chosen for illustration without departing from the spirit and scope of the invention. Specifically, it will be apparent to one of ordinary skill in the art that the device of the present invention could be implemented in several different ways and the apparatus disclosed above is only illustrative of the preferred embodiment of the invention and is in no way a limitation.

Claims

What is claimed is:

1. A method of communicating data packets in a wireless network, wherein the method comprises steps of:

a. receiving a first data packet wherein the first data packet is received according to a first rate of data communication;

b. receiving a second data packet wherein the second data packet is received according to a second rate of data communication and wherein the step of receiving the second data packet is performed simultaneously with the step of receiving the first data packet;

c. time division multiplexing the first data packet and the second data packet to a radio frame; and

d. communicating the radio frame via a wireless link wherein the radio frame is communicated at a third rate of data communication wherein the third rate of data communication is equal to at least a sum of the first rate of data communication and the second rate of data communication.

2. The method according to claim 1 further comprising a step of buffering the first data packet prior to performing the step of time division multiplexing wherein the step of buffering the first data packet synchronizes the first data packet to the radio frame.

3. The method according to claim 2 further comprising a step of buffering the second data packet prior to providing the second data packet to the radio framer wherein the step of buffering the second data packet synchronizes the second data packet to the radio frame.

4. The method according to claim 3 wherein the first and second data packets are received from an Ethernet local area network.

5. The method according to claim 3 wherein the first data packet is a 100 mega-bits per second (Mbps) Fast Ethernet data packet.

6. The method according to claim 5 wherein the second data packet is a 10 Mbps Ethernet data packet.

7. The method according to claim 1 further comprising steps of:
   a. receiving a third data packet; and
   b. time division multiplexing the third data packet to the radio frame.

8. The method according to claim 1 further comprising a step of encrypting the first data packet prior to performing the step of time division multiplexing.

9. A method of communicating data packets in a wireless network, wherein the method comprises steps of:
   a. receiving a first Fast Ethernet data packet into a first media access control (MAC) unit wherein the first Fast Ethernet data packet is received at a rate of 100 mega-bits per second (Mbps);
   b. receiving a second Fast Ethernet data packet into a second MAC unit wherein the second Fast Ethernet data packet is received at a rate of 100 Mbps and wherein the step of receiving the second Fast Ethernet data packet is performed simultaneously with the step of receiving the first Fast Ethernet data packet;
   c. providing the first Fast Ethernet data packet and the second Fast Ethernet data packet to a radio framer according to time division multiplexing thereby forming a time division multiplexed radio frame; and
   d. communicating the time division multiplexed radio frame via a wireless link wherein the time division multiplexed radio frame is communicated at a rate of at least 200 Mbps.

10. The method according to claim 9 wherein the first Fast Ethernet data packet is received from an Ethernet local area network coupled to the first MAC unit.

11. The method according to claim 9 further comprising steps of:

a. receiving a third Fast Ethernet data packet into a third MAC unit wherein the third Fast Ethernet data packet is received at a rate of 100 Mbps; and

b. providing the third Fast Ethernet data packet to the radio framer according to time division multiplexing.

12. The method according to claim 11 wherein the time division multiplexed radio frame is communicated at a rate of at least 300 Mbps.

13. The method according to claim 9 further comprising a step of buffering the first Fast Ethernet data packet in the first MAC unit prior to providing the first Fast Ethernet data packet to the radio framer.

14. The method according to claim 13 wherein the step of buffering the first Fast Ethernet data packet synchronizes the first Fast Ethernet data packet to the radio frame.

15. The method according to claim 14 further comprising a step of buffering the second Fast Ethernet data packet in the second MAC unit prior to providing the second Fast Ethernet data packet to the radio framer wherein the step of buffering the second Fast Ethernet data packet synchronizes the second Fast Ethernet data packet to the radio frame.

16. The method according to claim 9 further comprising a step of encrypting the first Fast Ethernet data packet prior to performing the step of providing the first Fast Ethernet data packet to the radio framer.

17. The method according to claim 9 further comprising a step of receiving an Ethernet data packet into the first MAC unit wherein the Ethernet data packet is received at a rate of 10 Mbps.

18. A terminal for a wireless link in a metropolitan area, the terminal comprising:

a. a first data packet receiver for receiving data packets for communication over a wireless link;

b. a second data packet receiver for receiving data packets for communication over the wireless link;

c. a multiplexer having a first input, a second input and an output wherein the first input is coupled to receive the data packets from the first data packet receiver and wherein the second input is coupled to receive the data packets from the second data packet receiver and wherein the output of the multiplexer provides time-division multiplexed data;

d. a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multplexed data according to radio frames; and

e. a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link.

19. The terminal according to claim 18 wherein the first data packet receiver is a first media access control (MAC) unit.

20. The terminal according to claim 19 wherein the first MAC unit further comprises:

a. a first rate control unit; and

b. a first rate buffer coupled to the first rate control unit for temporarily storing data packets received by the first MAC unit wherein the data packets are provided to the first input of the multiplexer from the first rate buffers.

21. The terminal according to claim 20 wherein the first MAC unit further comprises a first data encryption apparatus coupled to the first rate buffer.

22. The terminal according to claim 19 wherein the first MAC unit comprises a first data packet switch having a 100 mega-bits per second (Mbps) port wherein the first data packet switch is coupled to the rate control unit.

23. The terminal according to claim 22 wherein the first data packet switch is a layer-two switch.

24. The terminal according to claim 22 wherein the first data packet switch is a layer-three switch.

25. The terminal according to claim 22 wherein the first data packet switch further comprises a 10 Mbps port.

26. The terminal according to claim 22 wherein the 100 Mbps port receives data packets from a local area network coupled to the terminal.

27. The terminal according to claim 19 wherein the second data packet receiver is a second MAC unit.

28. The terminal according to claim 27 wherein the first MAC unit comprises a first data packet switch having a 100 Mbps port and wherein the second MAC unit comprises a second data packet switch having a 100 Mbps port.

29. The terminal according to claim 28 wherein the first data packet switch and the second data packet switch are each a layer-two switch.

30. The terminal according to claim 28 wherein the first MAC unit further comprises:

a. a first rate control unit coupled to the first data packet switch; and

b. a first rate buffer coupled to the first rate control unit for temporarily storing data packets received by the first data packet switch wherein the data packets are provided to the first input of the multiplexer from the first rate buffers.

31. The terminal according to claim 30 wherein the second MAC unit further comprises:

a. a second rate control unit coupled to the second data packet switch; and

b. a second rate buffer coupled to the second rate control unit for temporarily storing data packets received by the second data packet switch wherein the data packets are provided to the second input of the multiplexer from the second rate buffers.

32. The terminal according to claim 28 wherein the first MAC unit further comprises a first data encryption apparatus coupled to the first data packet switch.

33. The terminal according to claim 32 wherein the second MAC unit further comprises a second data encryption apparatus coupled to the second data packet switch.

34. A terminal for a wireless link in a metropolitan area, the terminal comprising:

a. a first media access control (MAC) unit for receiving Fast Ethernet data packets at a rate of 100 mega-bits per second (Mbps) for communication over a wireless link;

b. n-1 additional MAC units for receiving Fast Ethernet data packets at a rate of 100 Mbps for communication over the wireless link;

c. a multiplexer having n inputs, wherein each input is coupled to receive the data packets from a corresponding one of the first MAC unit and the n-1 additional MAC units and wherein the output of the multiplexer provides time-division multiplexed data;

d. a packet formatting apparatus coupled to the output of the multiplexer for formatting the time division multplexed data according to radio frames; and

e. a wireless transceiver coupled to the packet formatting apparatus for communicating the radio frames over a wireless link wherein the wireless link has a maximum bandwidth capacity of at least n times 100 Mbps.

35. The terminal according to claim 34 wherein each of the first MAC unit and the n-1 additional MAC units further comprise a rate control unit and a rate buffer coupled to the corresponding rate control unit for temporarily storing data packets received by the corresponding MAC unit prior to providing them to a corresponding one of the inputs of the multiplexer.

36. The terminal according to claim 35 wherein the first MAC unit and the n-1 additional MAC units further comprise an encryption apparatus coupled to the rate buffer of the corresponding MAC unit for encrypting data packets received by the corresponding MAC unit.

37. The terminal according to claim 34 wherein the first MAC unit comprises a first data packet switch having a 100 Mbps port.

38. The terminal according to claim 37 wherein the first data packet switch is a layer-two switch.

39. The terminal according to claim 37 wherein the first data packet switch is a layer-three switch.

40. The terminal according to claim 37 wherein the first data packet switch further comprises a 10 Mbps port.

41. The terminal according to claim 37 wherein the first MAC unit further comprises:

a. a first rate control unit coupled to the first data packet switch; and

b. a first rate buffer coupled to the first rate control unit for temporarily storing data packets received by the first data packet switch wherein the data packets are provided to the first input of the multiplexer from the first rate buffers.

42. The terminal according to claim 37 wherein each of the n-1 additional MAC units comprises a corresponding data packet switch having a 100 Mbps port.

43. The terminal according to claim 42 wherein each of the first MAC unit and the n-1 additional MAC units further comprises a rate control unit coupled to the corresponding data packet switch and a rate buffer coupled to the corresponding rate control unit for temporarily storing data packets prior to providing them to a corresponding one of the inputs of the multiplexer.

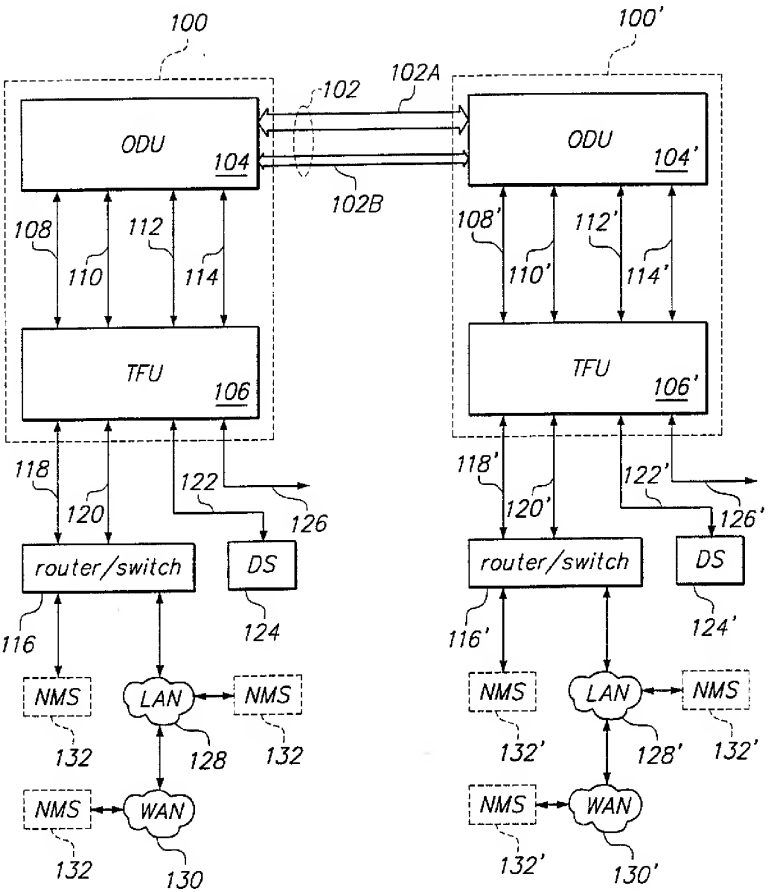

100
100'
102
102A
102B
ODU
104
ODU
104'
108
110
112
114
108'
110'
112'
114'
TFU
106
TFU
106'
118
120
122
126
118'
120'
122'
126'
router/switch
DS
router/switch
DS
116
124
116'
124'
NMS
LAN
NMS
NMS
LAN
NMS
132
128
132
132'
128'
132'
NMS
WAN
NMS
WAN
132
130
132'
130'

FIG. 1

FIG. 2A

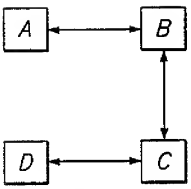


FIG. 2B

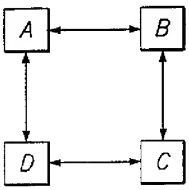


FIG. 2C

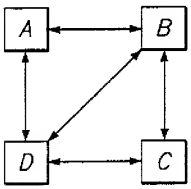


FIG. 2D

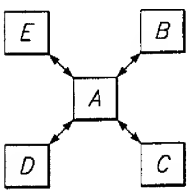


FIG. 2E

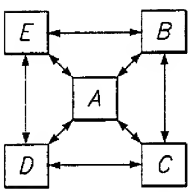


FIG. 2F

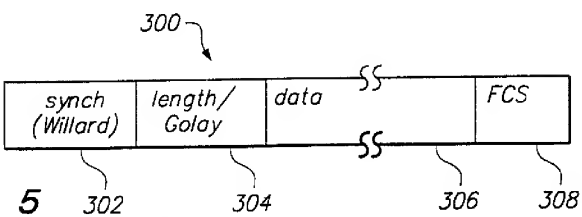


FIG. 5

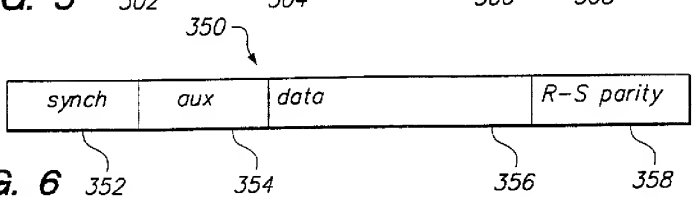


FIG. 6

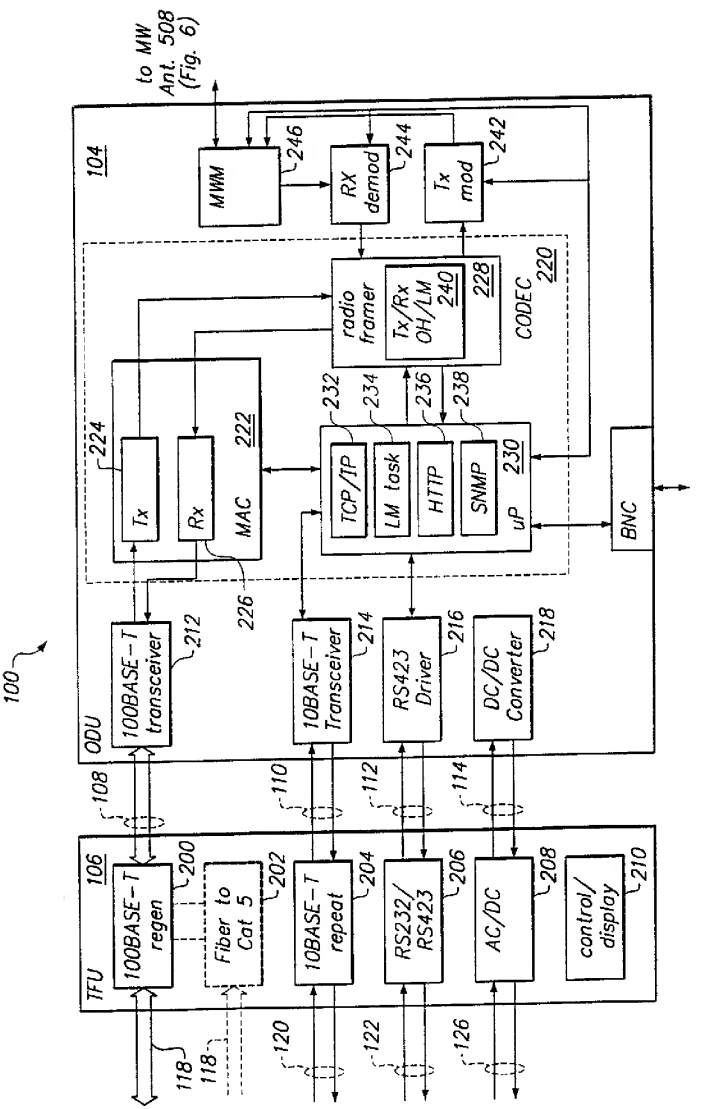

100
ODU
104
to MW Ant. 508 (Fig. 6)
MWM
246
RX demod
244
Tx mod
242
radio framer
Tx/Rx OH/LM
240
228
CODEC
220
224
Tx
Rx
MAC
222
226
232
234
236
238
TCP/IP
LM task
HTTP
SNMP
uP
230
BNC
100BASE-T transceiver
212
10BASE-T Transceiver
214
RS423 Driver
216
DC/DC Converter
218
108
110
112
114
TFU
106
100BASE-T regen
200
Fiber to Cat 5
202
10BASE-T repeat
204
RS232/ RS423
206
AC/DC
208
control/ display
210
118
118
120
122
126

FIG. 3

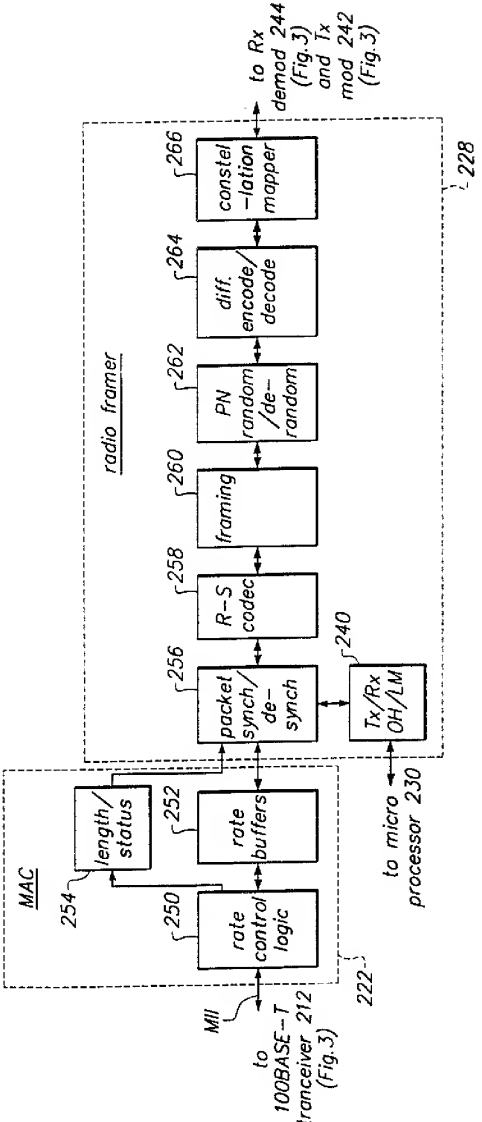

MAC
length/ status
254
rate buffers
252
rate control logic
250
MII
to 100BASE-T tranceiver 212 (Fig.3)
222
to micro processor 230
radio framer
packet synch/ de-synch
256
R-S codec
258
framing
260
PN random /de-random
262
diff. encode/ decode
264
constel -lation mapper
266
Tx/Rx OH/LM
240
228
to Rx demod 244 (Fig.3) and Tx mod 242 (Fig.3)

FIG. 4

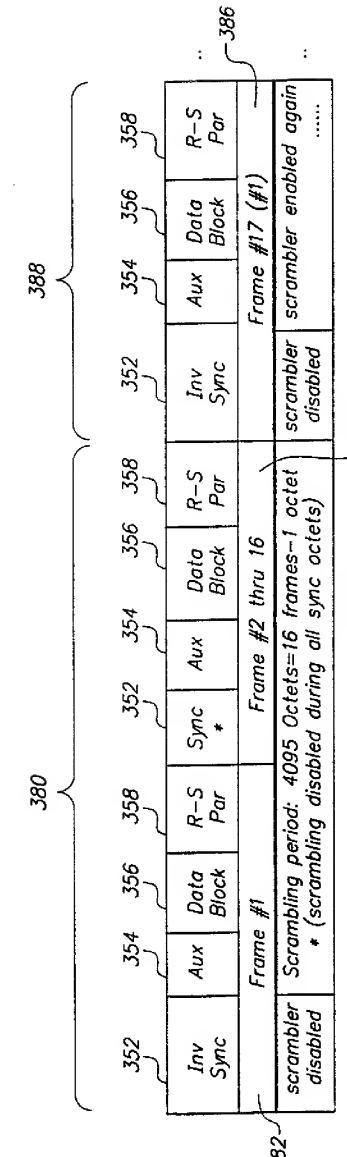

380
388
352
354
356
358
Inv Sync
Aux
Data Block
R-S Par
Sync *
Frame #1
Frame #2 thru 16
Frame #17 (#1)
scrambler disabled
scrambler enabled again .....
Scrambling period: 4095 Octets=16 frames-1 octet * (scrambling disabled during all sync octets)
382
384
386

FIG. 7

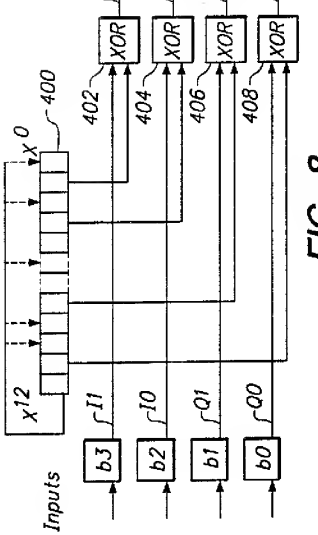

262
X^12
X^0
400
Inputs
b3
b2
b1
b0
I1
I0
Q1
Q0
402
404
406
408
XOR
I1'
I0'
Q1'
Q0'
from framing block 258 (Fig. 4)
to diff. decode/ encode 262 (Fig. 4)

FIG. 8

```
Quad  = 2*I1'+Q1';          - Map Quadrant Tag [0 1 2 3]
Phi   = [0 1 3 2] ;         - to Angle = [0 1 2 3]
Angle = Phi(Quad)
Sum   = (Sum+Angle)modulo 4 ;
I1"   = bit 1 of Sum ;  I0"   = I0';
Q1"   = bit 0 of Sum ;  Q0"   = Q0';
```

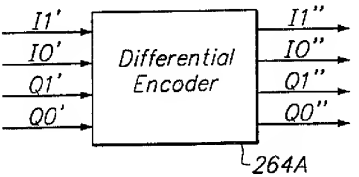


FIG. 9

```
Angle = 2*RxIs'+ RxQs' ;
Phi'  = [0 1 3 2] ;
Diff  = (Phi'(Angle)-Phi0) modulo 4 ;
Phi0  = Phi'(Angle) ;
RxIs  = bit 1 of Phi'(Diff) ;  RxIm = RxIm' ;
TxIs  = bit 0 of Phi'(Diff) ;  RxQm = RxQm' ;
```

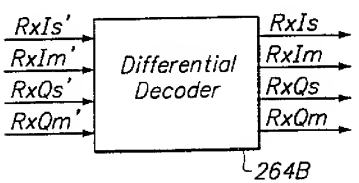


FIG. 10

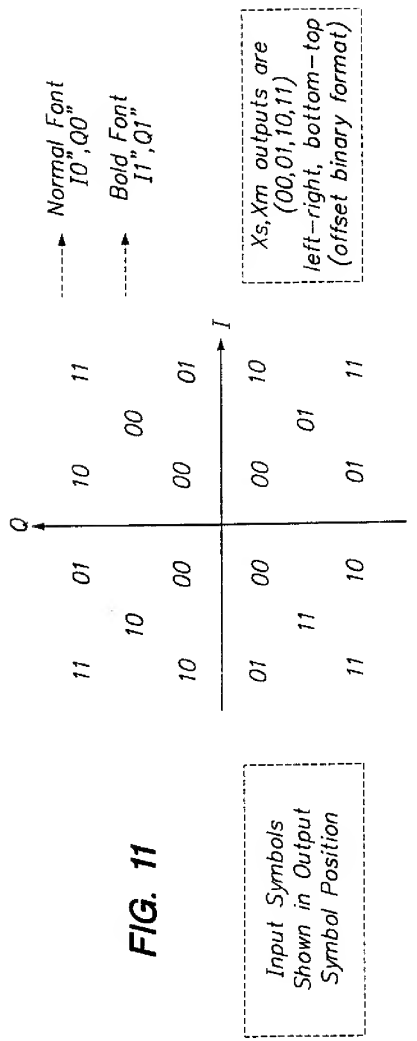

Q
I
Normal Font
I0",Q0"
Bold Font
I1",Q1"
Xs,Xm outputs are
(00,01,10,11)
left-right, bottom-top
(offset binary format)
Input Symbols
Shown in Output
Symbol Position
11 01 10 11
10 00 00 01
01 00 00 10
11 10 01 11
10
11
00
01

FIG. 11

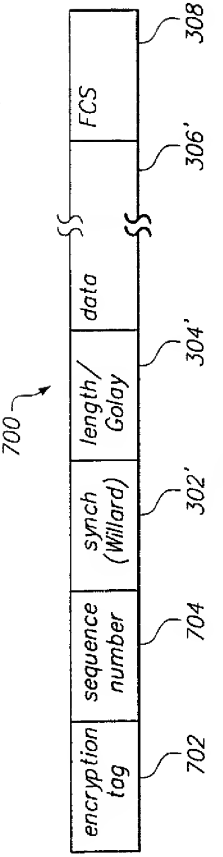

700
encryption tag
sequence number
synch (Willard)
length/ Golay
data
FCS
702
704
302'
304'
306'
308'

FIG. 17

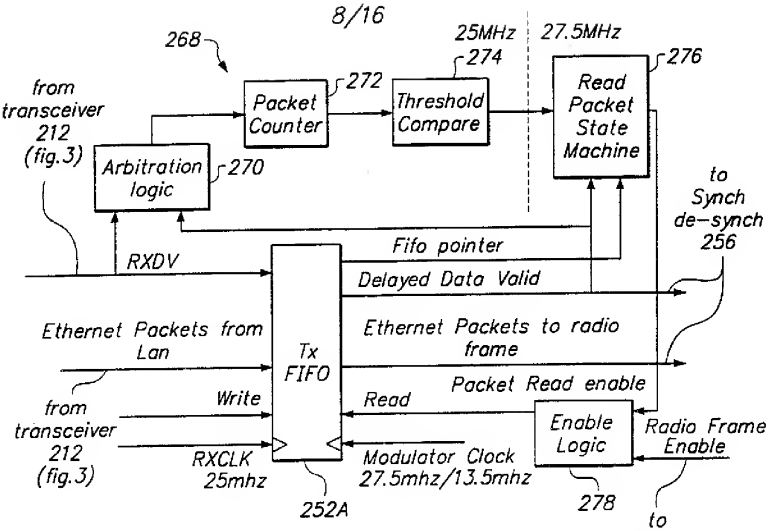

268
25MHz
27.5MHz
274
276
from transceiver 212 (fig.3)
Packet Counter
272
Threshold Compare
Read Packet State Machine
Arbitration logic
270
to Synch de-synch 256
RXDV
Fifo pointer
Delayed Data Valid
Ethernet Packets from Lan
Tx FIFO
Ethernet Packets to radio frame
Packet Read enable
from transceiver 212 (fig.3)
Write
Read
Enable Logic
Radio Frame Enable
RXCLK 25mhz
Modulator Clock 27.5mhz/13.5mhz
252A
278
to Synch de-synch 256

FIG. 12

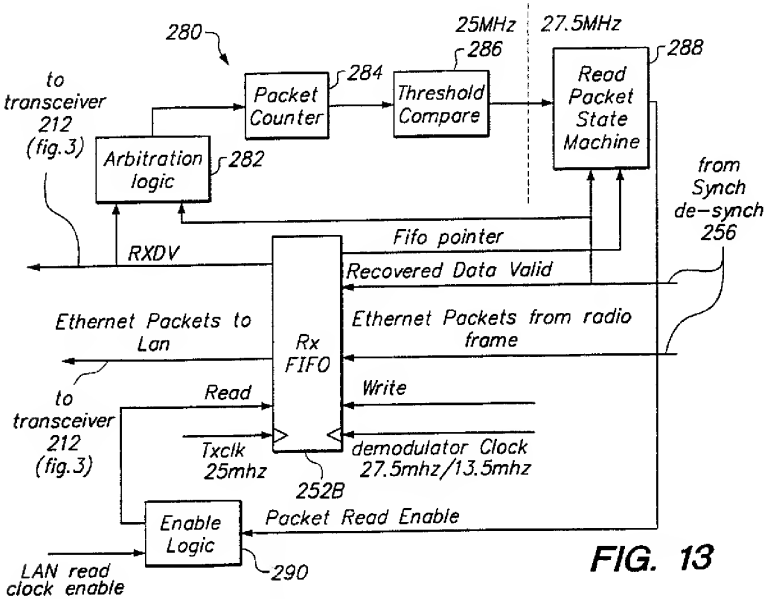

280
25MHz
27.5MHz
286
288
to transceiver 212 (fig.3)
Packet Counter
284
Threshold Compare
Read Packet State Machine
Arbitration logic
282
from Synch de-synch 256
RXDV
Fifo pointer
Recovered Data Valid
Ethernet Packets to Lan
Rx FIFO
Ethernet Packets from radio frame
to transceiver 212 (fig.3)
Read
Write
Txclk 25mhz
demodulator Clock 27.5mhz/13.5mhz
252B
Enable Logic
Packet Read Enable
LAN read clock enable
290

FIG. 13

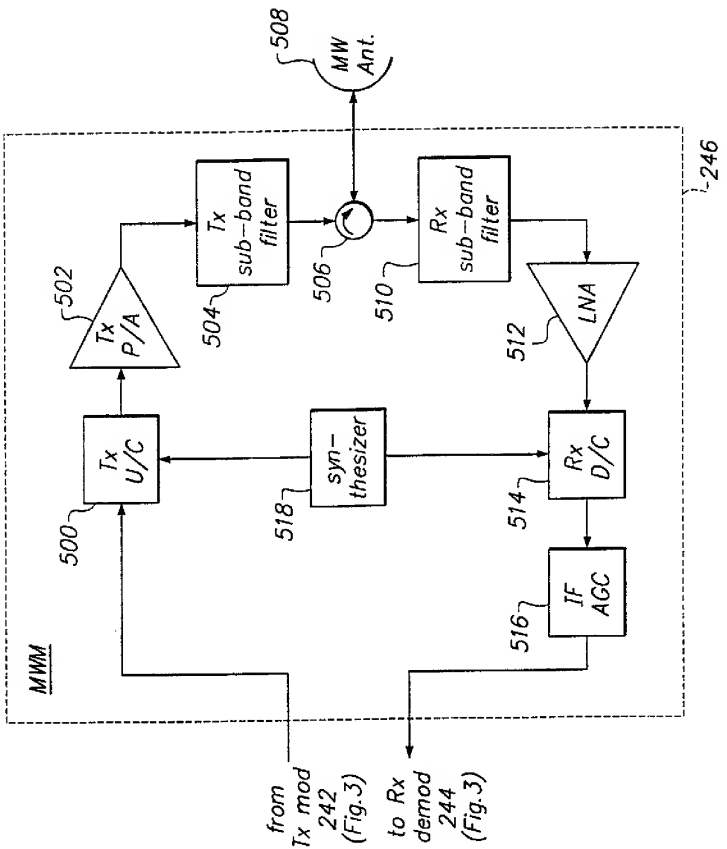

MWM
246
508
MW Ant.
Tx sub-band filter
Rx sub-band filter
506
502
Tx P/A
504
510
LNA
512
Tx U/C
syn-thesizer
Rx D/C
500
518
514
IF AGC
516
from Tx mod 242 (Fig.3)
to Rx demod 244 (Fig.3)

FIG. 14

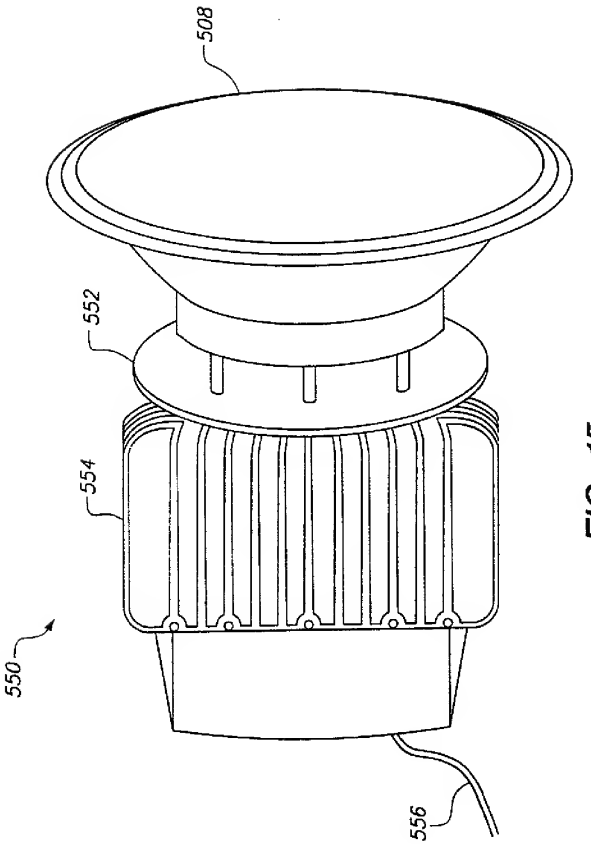


FIG. 15

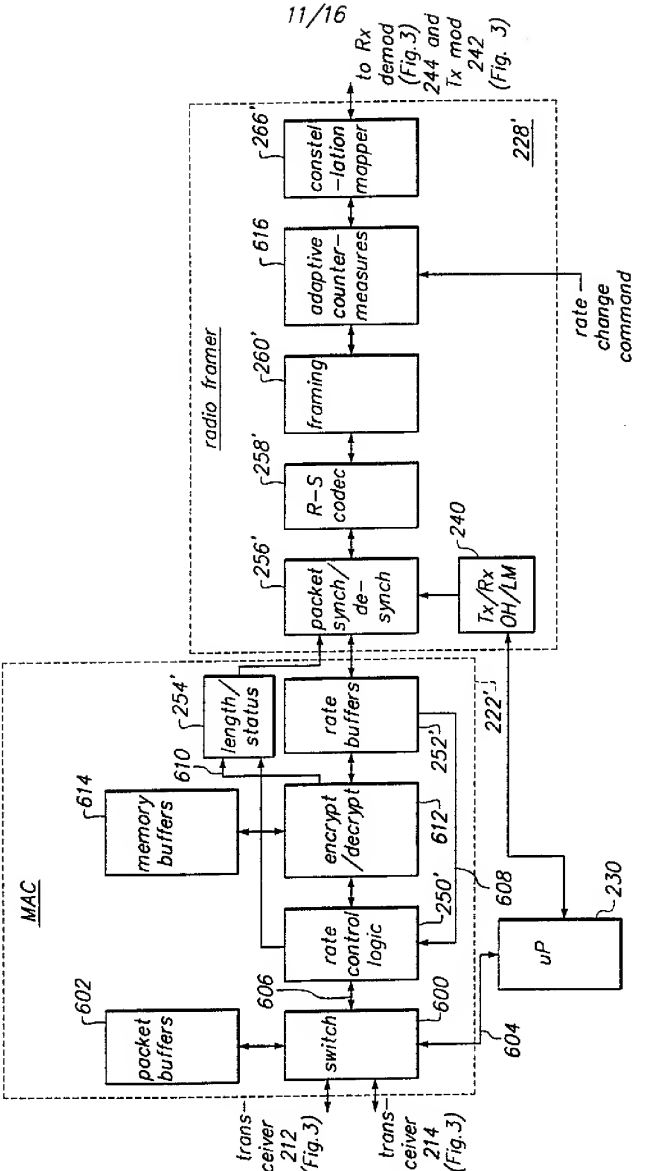
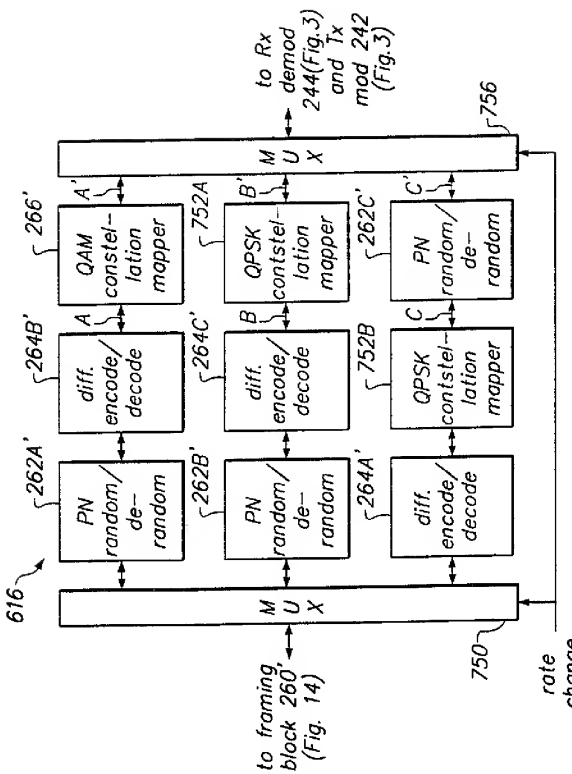

to Rx demod (Fig.3) 244 and Tx mod 242 (Fig. 3)
228'
radio framer
MAC
constel-lation mapper
266'
adaptive counter-measures
616
framing
260'
R-S codec
258'
packet synch/de-synch
256'
Tx/Rx OH/LM
240
rate change command
length/status
254'
rate buffers
252'
encrypt/decrypt
612
rate control logic
250'
memory buffers
614
610
packet buffers
602
switch
606
600
604
uP
608
230
222'
to trans-ceiver 212 (Fig.3)
to trans-ceiver 214 (Fig.3)

FIG. 16



A: data rate = 4 bits/symbol, symbol rate= 27.5 Msymbols (mega-symbols)/second
A': data rate = 4 bits/symbol, symbol rate= 27.5 Msymbols/second
B: data rate = 2 bits/symbol, symbol rate= 27.5 Msymbols/second
B': data rate = 2 bits/symbol, symbol rate= 27.5 Msymbols/second
C: data rate = 2 bits/symbol, symbol rate= 3.4375 Msymbols/second
C': data rate = 2 bits/symbol, symbol rate= 27.5 Msymbols/second

FIG. 18

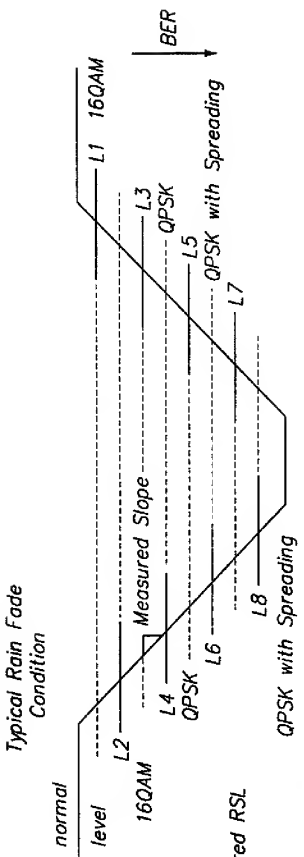

Typical Rain Fade Condition
normal
level
16QAM
Measured RSL
Time
L1 16QAM
L2
Measured Slope
L3
QPSK
L4
QPSK
L5
QPSK with Spreading
L6
L7
L8
QPSK with Spreading
BER

FIG. 19

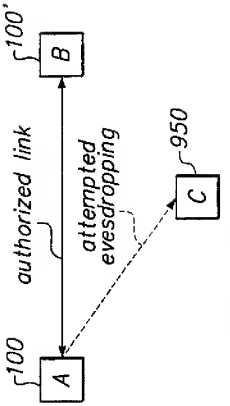

100
A
authorized link
100'
B
attempted evesdropping
950
C

FIG. 22

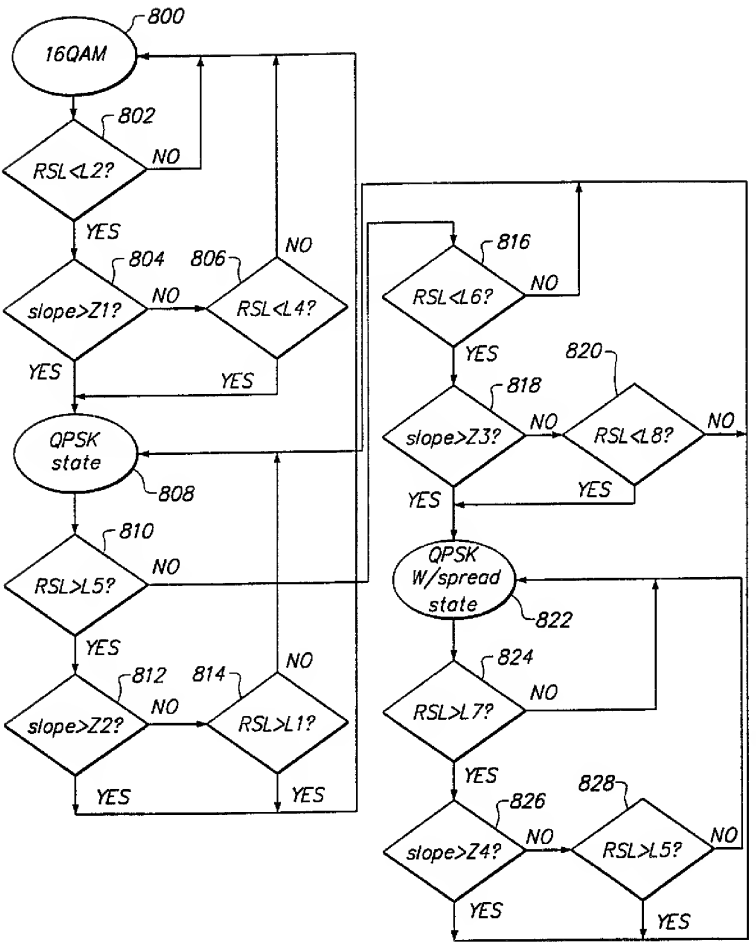

800
16QAM
802
RSL<L2?
NO
YES
804
806
NO
slope>Z1?
NO
RSL<L4?
YES
YES
QPSK state
808
810
RSL>L5?
NO
YES
812
814
NO
slope>Z2?
NO
RSL>L1?
YES
YES
816
RSL<L6?
NO
YES
820
818
slope>Z3?
NO
RSL<L8?
NO
YES
YES
QPSK W/spread state
822
824
RSL>L7?
NO
YES
828
826
slope>Z4?
NO
RSL>L5?
NO
YES
YES

FIG. 20

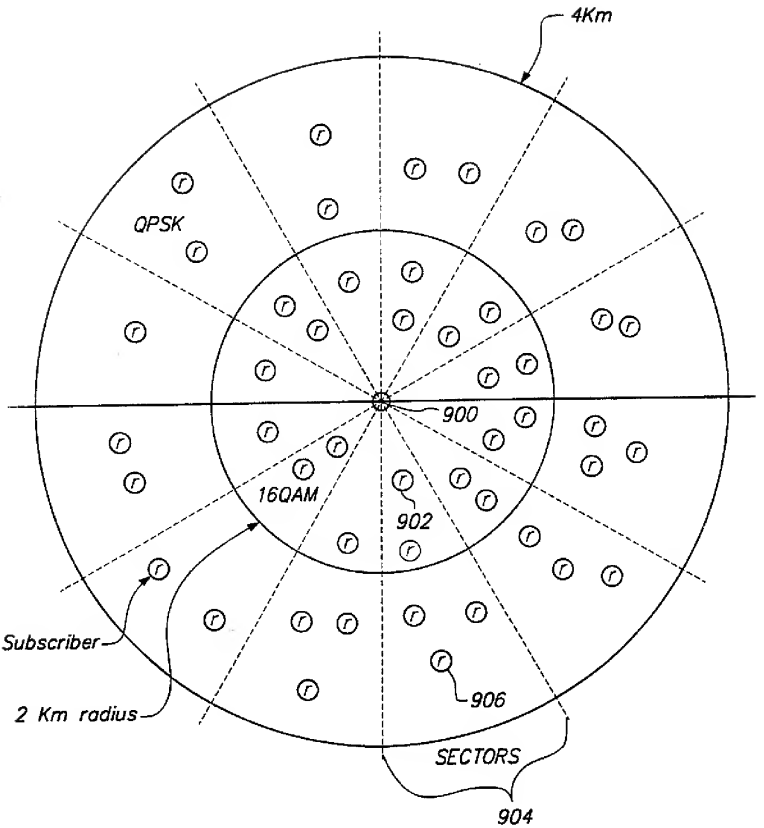

4Km
QPSK
900
16QAM
902
Subscriber
2 Km radius
906
SECTORS
904

FIG. 21

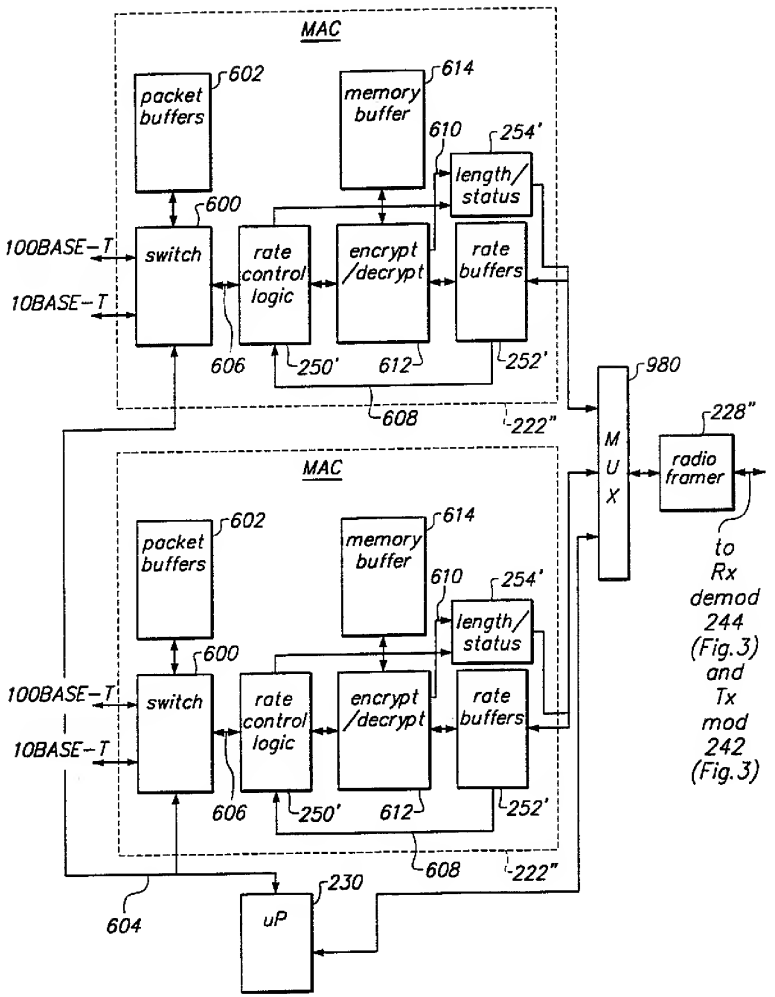

MAC
packet buffers
602
memory buffer
614
610
254'
length/ status
600
100BASE-T
10BASE-T
switch
rate control logic
encrypt /decrypt
rate buffers
606
250'
612
252'
608
222"
980
M U X
228"
radio framer
to Rx demod 244 (Fig.3) and Tx mod 242 (Fig.3)
MAC
packet buffers
602
memory buffer
614
610
254'
length/ status
600
100BASE-T
10BASE-T
switch
rate control logic
encrypt /decrypt
rate buffers
606
250'
612
252'
608
222"
604
uP
230

FIG. 23

INTERNATIONAL SEARCH REPORT

Intr tional Application No
PCT/US 99/11137

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04L12/46 H04B7/24

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 313 461 A (AHL KARL-AXEL ET AL) 17 May 1994 (1994-05-17) column 1, line 5 - line 61	1,7,18
Y	column 2, line 42 - line 56 column 5, line 3 - line 35 column 6, line 31 - line 34	2-4,8, 19,27
A	column 10, line 24 - line 30 claim 1; figures 3,5 --- -/--	5,6, 9-12,17, 22-26, 28,29, 34, 37-40,42

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Data of the actual completion of the international search	Date of mailing of the international search report
22 September 1999	11/10/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Blanco Cardona, P

3

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 975 906 A (ASANO MICHIO ET AL) 4 December 1990 (1990-12-04) abstract column 4, line 20 - line 32	2-4,19, 27
A	column 6, line 8 - line 12 column 8, line 15 - line 57 column 11, line 43 - line 50 column 12, line 20 - line 32 column 12, line 60 - line 68 column 15, line 48 - line 50 figures 9,10	1,9,10, 13-15, 18,20, 22-26, 28-31, 34,35, 37-43
A	US 5 648 969 A (PASTERNAK ELIEZER ET AL) 15 July 1997 (1997-07-15) column 1, line 42 -column 2, line 13 column 3, line 60 - line 65 column 6, line 55 -column 7, line 42 figures 3,6,7,11	1-3,7,9, 10, 13-15, 18-20, 22-31, 34,35, 37-43
Y	US 5 303 303 A (WHITE ANDREW R) 12 April 1994 (1994-04-12) column 1, line 36 - line 43	8
A	column 5, line 15 - line 60 column 7, line 16 - line 21 figures 8,10	16,21, 32,33,36